Martin Aigner • Günter M. Ziegler

Proofs from THE BOOK

天書の証明

M. アイグナー●G.M. ツィーグラー
蟹江幸博…訳

Springer

シュプリンガー・フェアラーク東京

序文

ポール・エルデシュは好んで天書のことを話したものである．G.H. ハーディーの，醜い数学に恒久的な場などない，という断定に従って，神が数学の定理の完全な証明を書き残しておく天書のことを．エルデシュはこうも言っている．神を信じる必要はないが，数学者として，天書は信じるべきだと．何年か前，私たちは彼に，近似的なものでよいから最初の（そして非常に慎ましい）天書を書いてみてはと勧めてみた．彼はそのアイデアに熱中してしまい，そして彼の性格からして，直ちに仕事に取り掛かり，何ページも何ページも自分の提案で埋めていった．我々の本はエルデシュの 85 歳の誕生日のプレゼントとして 1998 年 3 月に世に出ることになっていた．1996 年夏のポールの不幸な死のために，共著者として彼の名を挙げなかった．その代わり，本書を彼の想い出に捧げる．



ポール・エルデシュ

天書に記される証明であるための定義というか特徴付けというものはない．ここで私たちが提供するものはすべて，きらめくようなアイデアや鋭い洞察や素晴らしい観察についての私たちの興奮を読者にわかち合って欲しいと思い，選んだ例である．我々の解説が不完全であっても，読者はこれを楽しんで欲しいものだ．選択は大いに，ポール・エルデシュ自身の影響を受けている．多くの話題が彼によって提案されたもので，多くの証明が直接彼まで辿れるものか，彼の優れた洞察によって正しく質問されたり正しい予想の形にされたことに起源を持つものである．そうした訳で，かなりの程度本書は，何を天書に記される証明とすべきかということについて，ポール・エルデシュの考え方を反映している．



「天書」

話題を選ぶ際に制限としたことは，この本の中のあらゆることを，大学数学の中でもある程度の技巧を習得済みの読者であれば読むことがで

きる設定にしたことである．少しの線形代数，基本的な解析や数論もいくらか，離散数学からの初等的な概念や考え方も健康に悪くない程度の量，それだけあればこの本にあるあらゆることを理解し楽しむことができるべきだとした．

私たちは，このプロジェクトについて私たちを助け支持してくれた多くの人々に大変感謝している．とりわけ，草稿の議論をしたセミナーの学生たち，ベンノ・アルトマン，ステファン・ブラント，ステファン・フェルスナー，エリ・グッドマン，トルステン・ヘルドマン，ハンス・ミールケに感謝する．本書を作成するための技術的な援助をしてくれた，マルグリット・バレット，クリスティアン・ブレスラー，エウゲニ・ゴーリロフ，マイケル・ジョスウィグ，エルケ・ポーズ，イョルグ・ランバウに感謝する．原稿を最初から最後まで読んでくれたトム・トロッターと，素敵な図を描いてくれたカール・H・ホフマンと，偉大な故ポール・エルデシュ自身にはとりわけ，大きな恩義を感じている．

ベルリン，1998 年 3 月

マルティン・アイグナー

ギュンター・M・ツィーグラー

第2版への序文

本書の初版は素晴らしい歓迎を受けた．さらに，普通でないほど多数の手紙を受け取った．その中には，コメント，訂正，より短い方法，別証や扱うべき新しい話題に対する興味深い示唆が含まれていた．(我々は**完全**な証明の記録に努めたのだが，我々の説明はそうではなかったということである.)

第2版の出版は，本書のこの新しい形を提示する機会になった．3つの章を付け加え，いくつかの章で実質的な改訂と新しい証明をし，些細な修正や改良をしたが，その多くは寄せられた示唆に基づいている．また,「13の球面の問題」に関する，初版の1つの章を削除した．その証明には詳細な議論が必要で，エレガントかつ簡潔な証明にはできないことがわかったからである．

手紙を書いて我々を助けてくれたすべての読者に，とりわけ，ステファン・ブラント，ユルゲン・エルストロット，ロジャー・ヒース=ブラウン，リー・L・キーナー，ハンフリード・レンツ，ジョン・ショールズ，ベルヌルフ・ヴァイスバッハ，ニコラ・プュシュ，クリスチァン・レベゥフそのほか**大勢の方**に感謝する．また，シュプリンガー・ハイデルベルクのルース・アレヴェルトとカール=フリードリッヒ・コッホ，シュプリンガー・ベルリンのクリストッフ・エイリッヒとトルシュテン・ヘルドマンの助力と支援に，そしていくつか見事な新しい図を描いてくれたカール・H・ホフマンに感謝する．

ベルリン，2000年9月

マルティン・アイグナー
ギュンター・M・ツィーグラー

日本語版への序文

英語版の原著がこのように素晴らしい歓迎を受けたので，我々の本が他の重要な言語に，特に強力な数学的伝統を持つ国々に翻訳されて欲しいものと思っていた．日本人の印象深い数学的貢献や日本美術の時代を超えた感覚を思うに，数学における美とエレガンスは特に日本の読者には気に入ってもらえるものと思う．

英語第2版に基づいた日本語版が出版されることになって，我々はとてもうれしく思っている．翻訳者の蟹江幸博氏に心から感謝する．そのすべての仕事，その頑張り，またこの努力につぎ込んだ技術に感謝する．我々は今から，日本の読者からの示唆やコメントの手紙を受け取ることを楽しみにしている．

ベルリン，2002年11月

マルティン・アイグナー
ギュンター・M・ツィーグラー

訳者まえがき

「天書」は英語では The Book であり，ヨーロッパの慣習の中ではキリスト教の聖書を指すことが多いが，本来は「唯一の書」という意味である．唯一の書に記録する価値があるものと言えば，美と真実しかない．そのうちの 1 巻「真実の書」が天書である．いかにも壮大な物言いではあるが，本書の本当の著者であるポール・エルデシュはそう思っていた．そうある筈だと思っていた．

おそらくは命の尽きることを予感したエルデシュは，天書を自分の目でみたいと思ったのに違いない．「君の頭は営業中かね」と言いながら，世界中の数学者を訪ねて回り，時間も気にせず共同研究を始めたというエルデシュの人となりは，最近日本でも出版された伝記『数を愛した男[1]』に詳しい．すべての生活を数学に捧げ，周りのすべてを数学に巻き込んだエルデシュが心の拠り所としたのが天書であった．天書を垣間見，それを書き写すこと，それがエルデシュの生涯でもあった．

「序文」にあるように著者たちがエルデシュに提案しなかったら，おそらくは本書は生まれなかっただろう．天書そのものでなくてよい，その近似でもよいから，という提案はエルデシュにとって新鮮な驚きだっただろう．その驚きに打たれ，すぐさま作業に取り掛かったが，それを仕上げないうちに旅先のワルシャワでセミナーの途中に倒れ，病院に運ばれて亡くなった．

著者たちはエルデシュの遺志を継いで，本書を完成した．その経緯といい，内容といい，初版が出版された 1998 年に開かれたベルリンの国際

---

[1] 日本語版は，草思社から『放浪の天才数学者エルデシュ』（ポール・ホフマン著，平石律子訳）として出版されている．

数学者会議 (ICM) では大変な評判だったと言う．日本でもその秋の数学会の折，書籍展示場に本書はあった．それを見た途端，ぜひ早急に訳すべきだと編集者に話をした．そして，その方向に話は進んだのだが，一方で原著者の方は修正刷りを用意しており，次の年には第 2 版を出す予定でいるという．初版を数章訳し終わっていたが，第 2 版を待ってからの方がよいというのが出版社の判断で，そういうことになった．

第 2 版の出版は思ったよりも時間が掛かり，2000 年の末になった.「第 2 版への序文」にあるように大幅な変更があった．第 4 章の証明が全く別のものに変わっていたのは残念な気がした．訳してあった中で一番気に入っていた証明であった．また，使われていた図は本文中唯一のカラー図版だったので，著者たちにも特にお気に入りだった筈なのだが．確かに，第 2 版の証明はより初等的でわかりやすくなっている．著者たちのよりよいものを求める気持ちがそうさせたのだろう．エルデシュならそうしただろう，と著者たちは考えたのに違いない．

日本語版の出版を急ぐべきだと言っていた筈だったが，第 2 版が手元に届いた頃は別の仕事で手一杯になっており，本書の翻訳に本格的に取り掛かったのは 2001 年の秋になってからであった．第 2 版は非常に練りあげられた仕上がりで，ミスプリントもほとんどなく，そのため結果として著者への連絡が遅くなってしまった．やっと一通り翻訳原稿が出来た頃に，若干のミスプリントの指摘と共に著者に挨拶の電子メールを出した．

それから一転，目の回る思いをすることになった．こちらの指摘の返事以外に，彼ら自身が気がついたミス，また内容や図の修正が送られてくる．矢継ぎ早で，昼過ぎに送ったメールの返事が，その日の夕方に届くことも稀ではなかった．彼らの指示が，手元の原著と符合しないことが時々起こる．その点を重ねて尋ねると，フランス語版が出版され，さらに色々な意見やコメントが著者に寄せられ，そのため，原著第 2 版の修正 2 刷りが今年出版されていたことがわかった．著者からの指示はそれからの異同ということになっていたのである．著者たちもどの文章がどの版のものか分明でないようで，修正 2 刷りを送ってくれることになった．それが届いたのが，日本語版の印刷予定の 2 週間前であった．一番修正箇所の多い第 6 章だけは，修正 2 刷りとメールでの指示によって訳し直したが，著者・訳者に気がつかない異同が他にもあるかも知れない．小さいものなら，増刷の都度修正していくつもりである．

著者は，この仕事を始めてからずっとこれに関わってきたと，訳者へのメールで言っている．数学の発展と共に，これでよいと思った証明に間違いが見つかることがある（実際，第2版で「定理になった」と書いてあることが修正2刷りでは「まだ未解決である」となっている箇所がある）．また，よりよい証明が見つかることがある．より広く，深い見方ができるようになる．その都度，著者たちは本書を書き直して行く．彼らの背中をエルデシュが押しているのである．だから，これは終わりのない作業である．訳者もその流れの中で翻弄されたし，これからもこれは続くことになるようだ．

さて，何にしても，発見とは多くの場合，事実について述べられるものと考えられている．数学的発見においても，ある事実を証明することよりも，その事実が成り立つことを「知った」ということの方が重要であるという言い方がされることが多い．それでも，フェルマーの最終定理のワイルズによる証明のニュースでもわかるように，数学では証明そのものが重要な事実であると考えられている．それが数学の，少し特異なありようである．本書に溢れんばかりの美しい証明たちは，まさにそのことの「証明」であると言えるのかも知れない．

本書は，エルデシュの熱情から始まり，それが2人の著者に燃え移り，拡大し純化し，さらに燃え広がり，いよいよ天書に近づいて行く．多くの読者が，改良を提案し，瑕疵（かし）を指摘する．予想であったものが定理になり，定理の適用範囲が増えて行く．公刊された論文で，会議で，インターネットのやり取りで，証明が益々洗練されて行く．著者は即座にそれを本書に取り入れて行く．「日本語版への序文」の終わりにある言葉も決して社交辞令ではなく，著者は本当に，読者からの指摘や提案を歓迎している．

日本語版の日本語の間違いは訳者に，数学的内容の間違いの指摘，改良の提案などは訳者または直接著者にメールで知らせて欲しい．メールが使えない場合は，手紙で知らせて頂いてもよい．

本書の内容は多岐にわたり，新しい結果も多く含まれ，訳語が確定していないものも少なくない．そのような場合，異論はあるだろうが，できるだけ日本数学会編の『数学辞典第3版』に準拠することにした．

「人名索引」についても少し断っておかないといけないことがある．本書には最近の人々も数多く登場しており，そういう人の現在の所属は，わ

からないことも多く，本書に記述した情報が既に意味を持たなくなっている可能性もある．その他，人名索引に記載されるべき情報をご存じの方は，訳者まで知らせて欲しい．また，訳者のホームページ（奥付参照）の中の本書のページに出版後の修正事項を掲載しておくので，そこで確認の上，本書の改善に資することならどんなことでも，訳者に知らせていただきたい．

個人情報はわからないが，エルデシュ数ならわかる人もいる．そういう人の場合だけ，エルデシュ数を記載した．エルデシュ数の定義は簡単で，エルデシュと共著の論文を書いた人のエルデシュ数が 1 である．さらに，エルデシュ数 $<n$ の人と共著論文を書けばエルデシュ数 $\leq n$ が与えられ，その最小数が個人のエルデシュ数である．本書はエルデシュ数 1 のアイグナーとエルデシュ数 2 のツィーグラーを著者とし，(現在は) エルデシュ数が ∞ の訳者の手によるものである．本書の内容の多くは，エルデシュと小さいエルデシュ数を持つ数学者によるものである[2]．

これほど多くの登場人物の中に日本人はたった 1 人，岩本義和氏だけである．論文発表当時の数学会の名簿にもなく，本書に引用された論文以外には文献検索でも見つからない．長い間探した結果，1ヶ月前にやっと電話インタヴューをすることができた．当該の論文は，当時大阪理工科大学といった現近畿大学の紀要に，卒業研究を先輩や同級生と同じように載せただけだと話されていた．本書の読者の中からも，岩本氏と同じように，天書に刻まれる業績を挙げられる人が出ることを祈念して，訳者のまえがきとしよう．

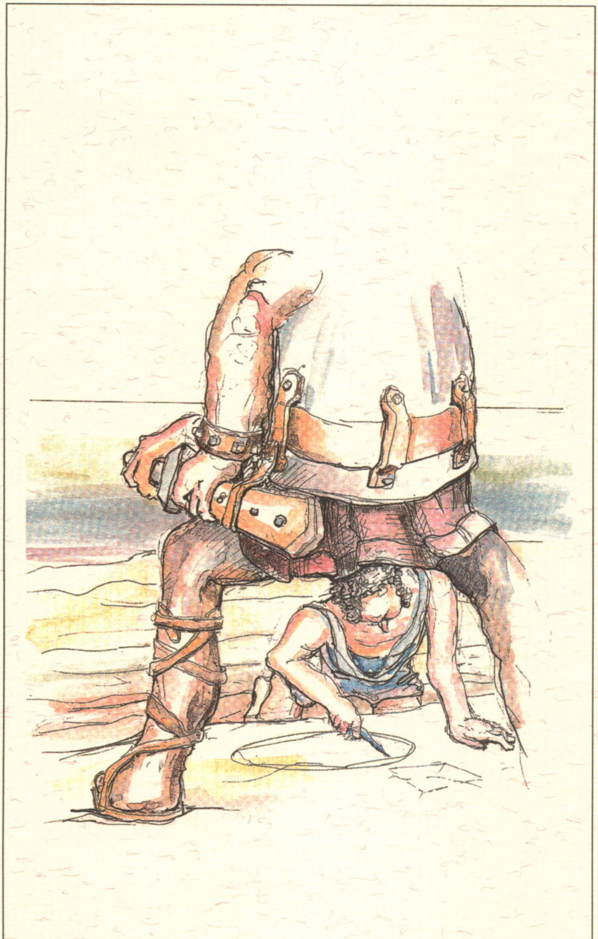
最後に，原稿の通読をして有益なコメントをしてくれた鳥羽商船高等専門学校の佐波学氏に，質問に迅速に答えてくれたツィーグラー氏に感謝する．

桑名にて，2002 年 11 月　　　　蟹江幸博

[2] エルデシュ数が 1 である数学者は 507 人存在する．エルデシュがいない今，その数は増えない．しかし，その人たちが生きている以上，エルデシュ数が 2 の数学者の数は増えるかも知れない．それらのエルデシュ数を管理するプロジェクトがある．そのホームページのアドレスは `http://www.oakland.edu/~grossman/erdoshp.html` である．そこに行けば，人名の年代順のリストもアルファベット順のリストも見ることができる．

目　次

数論



「無理数性と π」

（［訳註］剣に手をかけているローマの戦士に顔を向けようともせず図形を描き続けるアルキメデス.）

第1章　素数は無限：6つの証明

最初に挙げるのが自然なものと言えば，天書の証明でもおそらくは最も古い，次のものしかないだろう．それは通常ユークリッド（『原論』IX, 20）に帰されるもので，素数の列に終わりがないことを示すものである．

■ **ユークリッドの証明.** 素数の有限集合 $\{p_1, \ldots, p_r\}$ に対して，$n = p_1p_2 \cdots p_r + 1$ という数を考える．この n は素因数 p を持つ．しかし，p は p_i のどれでもない．p が p_i のどれかならば，p は n の約数でも $p_1p_2 \cdots p_r$ の約数でもあることになり，それゆえその差 $n - p_1p_2 \cdots p_r = 1$ の約数でもあるが，これはあり得ない．だから，有限集合 $\{p_1, \ldots, p_r\}$ はすべての素数の集合にはなり得ないのである． □

先に進む前に，記号をいくつか定めておく．$\mathbb{N} = \{1, 2, 3, \ldots\}$ は自然数の集合[1]，$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ は整数の集合，$\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ は素数の集合である．

これから，この他のいろいろな証明を示していく（証明自体はこの 6 つだけでなく，もっとたくさんある）が，我々と同じように読者もこれらを喜んでくれれば嬉しい．それらの証明は異なった観点からのものだが，そのすべてに共通な基本的アイデアがある．つまり，自然数はどんな限界をも超えて大きくなるものであり，あらゆる自然数 $n \geq 2$ は素因数を持つということである．この 2 つの事実のおかげで，$\mathbb{P}$ は無限集合になるのである．次の 3 つの証明は誰のものとも知れず伝承されたものであり，5 番目はハリー・フュルステンベルグの提案したもので，最後の証明はポール・エルデシュによるものである．

---

[1] ［訳註］以下では，$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\} = \mathbb{N} \cup \{0\}$ を使うことがある．

第 2 と第 3 の証明は，よく知られた特殊な数列を使うものである．

■ **第 2 の証明．** まず最初にフェルマー数 $F_n = 2^{2^n} + 1$ $(n = 0, 1, 2, \ldots)$ を考えよう．どんな 2 つのフェルマー数も互いに素であることを示す．そうすれば，素数は無限個ないといけないことになる．このために漸化式

$$\prod_{k=0}^{n-1} F_k \;=\; F_n - 2 \qquad (n \geq 1)$$

を示す．この式があれば，主張はすぐにわかる．実際，m が，たとえば F_k $(k < n)$ と F_n の約数ならば，m は 2 の約数でもあり，$m = 1, 2$ のどちらかになる．しかしフェルマー数はすべて奇数だから，$m = 2$ ということはあり得ない．

漸化式は n に関する帰納法で証明する．$n = 1$ のときは，$F_0 = 3$ であり $F_1 - 2 = 3$ である．あとは帰納法で，次のように計算される．

$$\prod_{k=0}^{n} F_k \;=\; \Big(\prod_{k=0}^{n-1} F_k\Big) F_n \;=\; (F_n - 2) F_n \;=$$

$$= (2^{2^n} - 1)(2^{2^n} + 1) \;=\; 2^{2^{n+1}} - 1 \;=\; F_{n+1} - 2. \qquad \square$$

■ **第 3 の証明．** $\mathbb{P}$ を有限集合とし，p を最大の素数とする．そこでいわゆる**メルセンヌ数** $2^p - 1$ を考え，$2^p - 1$ のどんな素因数 q も p より大きいことを示せば，望む結論が得られる．q を $2^p - 1$ を割る素数とすると，$2^p \equiv 1 \pmod{q}$ である．p は素数だから，これは体 $\mathbb{Z}_q$ の乗法群 $\mathbb{Z}_q \backslash \{0\}$ の中で 2 という元が位数 p であることを意味している．この群は $q - 1$ 個の元を持つ．ラグランジュの定理（余白の箱を見よ）から，あらゆる元の位数は群の大きさの約数であることがわかり，つまり $p \mid q - 1$ であって，したがって $p < q$ となる．$\square$

今度はやさしい微積分を使った証明を見よう．

■ **第 4 の証明．** $\pi(x) = \#\{p \leq x \;:\; p \in \mathbb{P}\}$ を実数 x 以下の素数の個数とする．大きくなる順に素数を並べて $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ とする．自然対数 $\log x$ は $\log x = \int_1^x \frac{1}{t} dt$ と定義されている．

そこで，$f(t) = \frac{1}{t}$ のグラフの下の面積を，上からの階段関数と比較する．(この方法については 14 ページの附録も見ること.) すると，$n \leq x < n+1$ に対しては

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \\ F_5 &= 641 \cdot 6700417 \end{aligned}$$

最初の方のフェルマー数．

ラグランジュの定理

G を有限（乗法）群，U をその部分群とすると，$|U|$ は $|G|$ を割る．

■ **証明．** 2 項関係

$$a \sim b :\Longleftrightarrow ba^{-1} \in U$$

を考える．群の公理から $\sim$ が同値関係であることがわかる．元 a を含む同値類はコセット

$$Ua = \{xa : x \in U\}$$

に一致する．明らかに $|Ua| = |U|$ なので，G は，すべての大きさが $|U|$ である同値類に分解される．それゆえ，$|U|$ は $|G|$ を割る．$\square$

U が巡回部分群 $\{a, a^2, \ldots, a^m\}$ という特殊な場合には，m ($a^m = 1$ を満たす最小の正整数，これを a の**位数**と言う）は群の大きさ $|G|$ を割る．

$$\log x \le 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}$$
$$\le \sum \frac{1}{m}$$

となる．ここで，和は，$p \le x$ を満たす素因数しか持たないようなすべての数 $m \in \mathbb{N}$ に関してとる．このような m は $\prod_{p \le x} p^{k_p}$ の形の積に**一意的に書く**ことができるので，上の最後の和は

$$\prod_{\substack{p \in \mathbb{P} \\ p \le x}} \Big(\sum_{k \ge 0} \frac{1}{p^k} \Big)$$

に等しい．内部の和は公比 $\frac{1}{p}$ の等比級数だから，

$$\log x \ \le \ \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{1}{1 - \frac{1}{p}} \ = \ \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{p}{p-1} \ = \ \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}$$

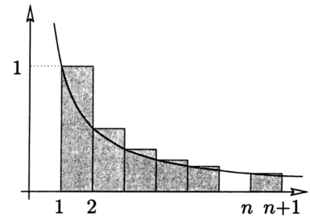
となる．$p_k \ge k+1$ は明らかだから，

$$\frac{p_k}{p_k - 1} \ = \ 1 + \frac{1}{p_k - 1} \ \le \ 1 + \frac{1}{k} \ = \ \frac{k+1}{k}$$

となるので，

$$\log x \ \le \ \prod_{k=1}^{\pi(x)} \frac{k+1}{k} \ = \ \pi(x) + 1$$

となる．$\log x$ が有界でないのは誰もが知っていることだから，$\pi(x)$ もまた有界でなく，したがって無限個の素数が存在するという結論が得られる．　□



関数 $f(t) = \frac{1}{t}$ の上からの階段関数．

■ **第5の証明．** 解析の次はトポロジーの番である！ 整数の集合 $\mathbb{Z}$ の上に次の奇妙な位相を考える．$a, b \in \mathbb{Z}, b > 0$ に対して

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$$

とおく．各集合 $N_{a,b}$ は両方向への無限等差数列である．そこで，集合 $O \subseteq \mathbb{Z}$ が**開集合**であることを，O が空集合であるか，あるいはあらゆる $a \in O$ に対して，$N_{a,b} \subseteq O$ を満たす $b > 0$ が存在するときとす

る．明らかに，開集合の和集合は開集合である．O_1, O_2 が開集合であり，$a \in O_1 \cap O_2$ に対して $N_{a,b_1} \subseteq O_1$ かつ $N_{a,b_2} \subseteq O_2$ であれば，$a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$ となる．だから，有限個の開集合の共通部分もまた開集合である．だから，この開集合族は $\mathbb{Z}$ の上にちゃんとした位相を定めている．

ここで次の2つの事実に注意する．

(A) 空でない開集合はすべて無限集合である．

(B) どんな集合 $N_{a,b}$ も閉集合である．



「平たい石を投げる，果てしなく．」

実際，第1の事実は定義からわかる．第2の事実については

$$N_{a,b} \;=\; \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$

という式によって，$N_{a,b}$ が開集合の補集合だから閉集合でもあることがわかる．

これまでのところ，素数はまだ出てきていない．しかし，実は出てきているのだ．どんな数 $n \neq 1, -1$ も，素因数 p を持っているから，$N_{0,p}$ に含まれ，結局

$$\mathbb{Z} \setminus \{1, -1\} \;=\; \bigcup_{p \in \mathbb{P}} N_{0,p}$$

となる．そこでもし $\mathbb{P}$ が有限集合なら，$\bigcup_{p \in \mathbb{P}} N_{0,p}$ は閉集合の有限和で（(B) による），したがって閉集合である．その結果，$\{1, -1\}$ が開集合になるが，これは (A) に矛盾する．　□

■ **第6の証明.** 最後の証明はかなり踏み込んだもので，素数が無限個あるというだけでなく，級数 $\sum_{p \in \mathbb{P}} \frac{1}{p}$ が発散することも示している．この重要な事実の最初の証明はオイラーによるものだが（それ自身興味深い），エルデシュによって考案された以下の証明には目を見張る美しさがある．

$p_1, p_2, p_3, \ldots$ は素数を大きくなる順に並べたもので，$\sum_{p \in \mathbb{P}} \frac{1}{p}$ が収束すると仮定する．すると，自然数 k で，$\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$ となるものがなくてはならない．$p_1, \ldots, p_k$ を小さい素数，$p_{k+1}, p_{k+2}, \ldots$ を大きい素数と呼ぶことにする．そうすると任意の自然数 N に対して

$$\sum_{i \geq k+1} \frac{N}{p_i} \quad < \quad \frac{N}{2} \tag{1}$$

となる．N_b を，少なくとも 1 つの大きい素数で割り切れる正の数 $n \leq N$ とし，N_s を，小さい素数しか約数としない正の数 $n \leq N$ の数とする．そこで，適当な N に対して

$$N_b + N_s \quad < \quad N$$

となることを示すことにする．これが示されると矛盾が得られるのは，$N_b + N_s$ は定義から N に等しいからである．

N_b を評価するために，$\left\lfloor \frac{N}{p_i} \right\rfloor$ が，p_i の倍数であるような正の整数 $n \leq N$ の個数を数えるものであることに注意する．それゆえ (1) により，

$$N_b \ \leq \ \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \ < \ \frac{N}{2} \tag{2}$$

となる．さて，N_s を考えよう．小さい素数しか素因数として持たないあらゆる $n \leq N$ を $n = a_n b_n^2$ の形に書く．ここで，a_n は 2 乗の部分がないようにとる．こうして，a_n は**異なる**小さな素数の積となるので，2 乗を含まない部分はちょうど 2^k 通りあることになる．さらに，$b_n \leq \sqrt{n} \leq \sqrt{N}$ だから，2 乗部分も高々 $\sqrt{N}$ 通りしか異なるものはないので，

$$N_s \quad \leq \quad 2^k \sqrt{N}$$

となる．(2) はどんな N に対しても成り立つので，$2^k \sqrt{N} \leq \frac{N}{2}$，つまり $2^{k+1} \leq \sqrt{N}$ となるような数 N を見つけることだけが残ったのだが，このためには $N = 2^{2k+2}$ とすればよい． □

参考文献

[1] B. アルトマン：『ユークリッド — 数学の創造』(*Euclid — The Creation of Mathematics*), Springer-Verlag, New York 1999[2].

[2] P. エルデシュ：「級数 $\sum \frac{1}{p}$ について」(*Über die Reihe* $\sum \frac{1}{p}$), Mathematica, Zutphen B **7** (1938), 1-2.

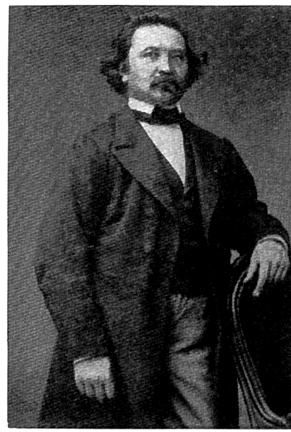
[2] ［訳註］日本語訳は，『数学の創造者 — ユークリッド原論の数学』（大矢健正訳，シュプリンガー・フェアラーク東京，2002）．

[3] L. オイラー：『無限解析入門』(*Introductio in Analysin Infinitorum*), Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8[3].

[4] H. フュルステンベルグ：「素数の無限性について」(*On the infinitude of primes*), Amer. Math. Monthly **62** (1955), 353.

3 ［訳註］日本語訳は,『オイラーの無限解析』（高瀬正仁訳，海鳴社，2001）.

第2章　ベルトランの仮説



ジョゼフ・ベルトラン

素数列 $2, 3, 5, 7, \ldots$ が無限列であることはすでにわかっている．この列の間隙の大きさも有界でない．それを見るには，$N = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p$ を $k+2$ より小さなすべての素数の積とし，k 個の数

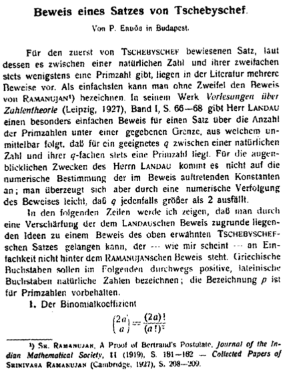
$$N+2,\ N+3,\ N+4,\ \ldots,\ N+k,\ N+(k+1)$$

のどれもが素数でないことに注意すればよい．なぜなら，$2 \leq i \leq k+1$ に対して，i は $k+2$ より小さな素因数を持つが，その素因数は N も割るので，$N+i$ を割るからである．このレシピに従えば，たとえば $k = 10$ に対しては，10 個の数

$$2312, 2313, 2314, \ldots, 2321$$

のどれも素数でないことがわかる．

しかし，素数列の間隙に対しては上界もあるのである．上界の中で有名なものは「次の素数までの間隙は探し始めるその数よりは大きくなれない」というものである．これは，ジョゼフ・ベルトランが予想し，$n < 3000000$ に対して実際に計算して確かめたので，ベルトランの仮説として知られている．パフヌートゥィ・チェビシェフは 1850 年に，すべての n に対する最初の証明をした．ずっと簡単な証明が，インドの天才ラマヌジャンによって与えられた．ここで与える天書の証明はポール・エルデシュによるものである．これは，エルデシュ19 歳の 1932 年に出版された，彼の最初の公刊論文に載っている．



Beweis eines Satzes von Tschebyschef.

Von P. Erdős in Budapest.

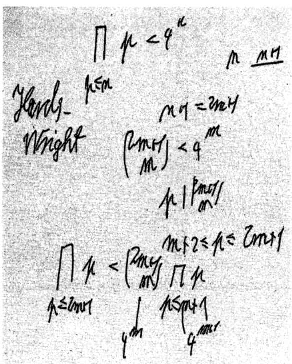
Für den zuerst von Tschebyschef bewiesenen Satz, laut dessen es zwischen einer natürlichen Zahl und ihrer zweifachen stets wenigstens eine Primzahl gibt, liegen in der Literatur mehrere Beweise vor. Als einfachsten kann man ohne Zweifel den Beweis von Ramanujan[1]) bezeichnen. In seinem Werk *Vorlesungen über Zahlentheorie* (Leipzig, 1927), Band I, S. 66—68 gibt Herr Landau einen besonders einfachen Beweis für einen Satz über die Anzahl der Primzahlen unter einer gegebenen Grenze, aus welchem unmittelbar folgt, daß für ein geeignetes q zwischen einer natürlichen Zahl und ihrer q-fachen stets eine Primzahl liegt. Für die augenblicklichen Zwecken des Herrn Landau kommt es nicht auf die numerische Bestimmung der im Beweis auftretenden Konstanten an; man überzeugt sich aber durch eine numerische Verfolgung des Beweises leicht, daß q jedenfalls größer als 2 ausfällt.

In den folgenden Zeilen werde ich zeigen, daß man durch eine Verschärfung der dem Landauschen Beweis zugrunde liegenden Ideen zu einem Beweis des oben erwähnten Tschebyschefschen Satzes gelangen kann, der — wie mir scheint — an Einfachkeit nicht hinter dem Ramanujanschen Beweis steht. Griechische Buchstaben sollen im Folgenden durchwegs positive, lateinische Buchstaben natürliche Zahlen bezeichnen; die Bezeichnung p ist für Primzahlen vorbehalten.

1. Der Binomialkoeffizient

$$\binom{2a}{a} = \frac{(2a)!}{(a!)^2}$$

1) Sr. Ramanujan, A Proof of Bertrand's Postulate, *Journal of the Indian Mathematical Society*, 11 (1919), S. 181—182 — *Collected Papers of Srinivasa Ramanujan* (Cambridge, 1927), S. 208—209.



ベルトランの仮説.
あらゆる $n \geq 1$ に対して，$n < p \leq 2n$ を満たす素数 p が存在する.

■ **証明.** 2 項係数 $\binom{2n}{n}$ の大きさを慎重に評価して，$n < p \leq 2n$ の範囲にどんな素因数もないのなら 2 項係数は「小さすぎる」ことになる，ということを示す．我々の議論は 5 段階に分かれる．

(1) まず，$n < 4000$ に対してベルトランの仮説を証明する．このために，4000 もの場合を確かめる必要はない．

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$

が素数列で，それぞれ 1 つ前の数の 2 倍より小さいことを確かめれば十分である（これを「ランダウのトリック」と言う）．それゆえ，$n < 4000$ に対して，あらゆる区間 $\{y : n < y \leq 2n\}$ はこの 14 個の素数の中の 1 つを含む．

(2) 次に

$$\prod_{p \leq x} p \;\leq\; 4^{x-1} \qquad \text{（すべての実数}x \geq 2\text{ に対して）} \qquad (1)$$

を証明する．ここで，これ以降使う記号として，上式の中の積は $p \leq x$ を満たすすべての**素数** p にわたってとることとする．この事実に対してここで示す証明は，これらの素数の個数に関する帰納法を使う．エルデシュの原論文の証明ではないが，これもエルデシュによるものであり（余白参照），まさに本物の天書の証明である． まず，q が $q \leq x$ を満たす最大の素数であれば，

$$\prod_{p \leq x} p = \prod_{p \leq q} p \qquad \text{かつ} \qquad 4^{q-1} \leq 4^{x-1}$$

であることに注意する．つまり，$x = q$ が素数の場合にだけ (1) を確かめればよい．$q = 2$ のときは「$2 \leq 4$」だから，奇素数 $q = 2m+1$ の場合に考えることにする．このときは積を分解して，

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p \leq 2m+1} p \;\leq\; 4^m \binom{2m+1}{m} \leq 4^m 2^{2m} \;=\; 4^{2m}$$

と計算する．この「1 行の計算」のどの部分も簡単にわかる．実際

$$\prod_{p\le m+1} p \ \le \ 4^m$$

は帰納法の仮定である．

$$\prod_{m+1<p\le 2m+1} p \ \le \ \binom{2m+1}{m}$$

という不等式は，$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ が整数であり，考えている素数はすべて分子 $(2m+1)!$ の素因数であって，分母 $m!(m+1)!$ には含まれないことを考えればわかる．最後に，

$$\binom{2m+1}{m} \ \le \ 2^{2m}$$

であることは，

$$\binom{2m+1}{m} \quad と \quad \binom{2m+1}{m+1}$$

が，和

$$\sum_{k=0}^{2m+1}\binom{2m+1}{k} = 2^{2m+1}$$

の中に現れる，2 つの（等しい！）項であることからわかる．

(3) ルジャンドルの定理（余白の箱を見よ）から，$\binom{2n}{n} = \frac{(2n)!}{n!n!}$ が素因数 p をちょうど

$$\sum_{k\ge 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right)$$

回だけ含んでいることがわかる．この和の各項は高々 1 である．というのは，

$$\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor \ < \ \frac{2n}{p^k} - 2\left(\frac{n}{p^k}-1\right) \ = \ 2$$

を満たす整数だからである．さらに，これらの項は $p^k > 2n$ のときは 0 になる．こうして，$\binom{2n}{n}$ は p を，

$$\sum_{k\ge 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) \ \le \ \max\{r : p^r \le 2n\}$$

ルジャンドルの定理

数 $n!$ は素因数 p をちょうど

$$\sum_{k\ge 1}\left\lfloor\frac{n}{p^k}\right\rfloor$$

回含む．

■ **証明.** $n! = 1\cdot 2\cdot 3\cdot\cdots\cdot n$ の因数のちょうど $\left\lfloor\frac{n}{p}\right\rfloor$ 個が p で割り切れ，これを数えると $\left\lfloor\frac{n}{p}\right\rfloor$ 個の p 因数が得られる．次に，$n!$ の $\left\lfloor\frac{n}{p^2}\right\rfloor$ 個の因数は p^2 でも割れ，これを数えると $n!$ の次の $\left\lfloor\frac{n}{p^2}\right\rfloor$ 個の素因数 p が得られる，などとなる． □

回だけ含んでいる．それゆえ，$\binom{2n}{n}$ を割る最大の p のベキは $2n$ より大きくない．とくに，$p > \sqrt{2n}$ を満たす素数 p は $\binom{2n}{n}$ には高々1回しか現れない．

さらに，エルデシュによると，これが証明の鍵になる事実なのだが，$\frac{2}{3}n < p \le n$ を満たす素数は決して $\binom{2n}{n}$ を割ることはない！ 実際，$3p > 2n$ からは（$n \ge 3$，それゆえ $p \ge 3$ に対して），$\frac{(2n)!}{n!n!}$ の分子の因数として現れる p の倍数が p と $2p$ の2つしかないのに，分母には p 因数が2つあるからである．

たとえば
$\binom{26}{13} = 2^3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 19 \cdot 23$
$\binom{28}{14} = 2^3 \cdot 3^3 \cdot 5^2 \cdot 17 \cdot 19 \cdot 23$
$\binom{30}{15} = 2^4 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 23 \cdot 29$
で見られるように，「非常に小さな」素因数 $p < \sqrt{2n}$ は $\binom{2n}{n}$ の中に高い次数で現れ得るが，$\sqrt{2n} < p \le \frac{2}{3}n$ ほどの「小さな」素数は高々1回しか現れず，$\frac{2}{3}n < p \le n$ という隙間にある素数はまったく現れない．

(4) さて，$\binom{2n}{n}$ の評価ができるようになった．$n \ge 3$ に対して，16ページの下からの評価を使えば，

$$\frac{4^n}{2n} \le \binom{2n}{n} \le \prod_{p \le \sqrt{2n}} 2n \cdot \prod_{\sqrt{2n} < p \le \frac{2}{3}n} p \cdot \prod_{n < p \le 2n} p$$

が得られ[1]，$p \le \sqrt{2n}$ を満たす素数 p は $\sqrt{2n}$ 個より多くないので，

$$4^n \le (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n} < p \le \frac{2}{3}n} p \cdot \prod_{n < p \le 2n} p \qquad (n \ge 3) \qquad (2)$$

が得られる．

(5) ここで，$n < p \le 2n$ を満たす素数 p が存在しないと仮定しよう．すると，(2) 式の最後の積は 1 である．(1) 式を (2) 式に代入すると，

$$4^n \le (2n)^{1+\sqrt{2n}} 4^{\frac{2}{3}n}$$

つまり

$$4^{\frac{1}{3}n} \le (2n)^{1+\sqrt{2n}} \qquad (3)$$

が得られるが，この式は n が十分大きくなると成り立たない！ 実際，$a + 1 < 2^a$（これは，帰納法によって，すべての $a \ge 2$ に対して成り立つ）という不等式を使えば，

$$2n = \left(\sqrt[6]{2n}\right)^6 < \left(\left\lfloor \sqrt[6]{2n} \right\rfloor + 1\right)^6 < 2^{6\left\lfloor \sqrt[6]{2n} \right\rfloor} \le 2^{6\sqrt[6]{2n}} \qquad (4)$$

---

[1] ［訳註］(3) で $\binom{2n}{n}$ の素因数 p が何回含まれ得るかが示してある．

が得られる．こうして，$n \geq 50$（このとき $18 < 2\sqrt{2n}$ である）に対し，(3) と (4) から，

$$2^{2n} \leq (2n)^{3\left(1+\sqrt{2n}\right)} < 2^{\sqrt[6]{2n}\left(18+18\sqrt{2n}\right)} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}$$

が得られる．これから，$(2n)^{1/3} < 20$ が得られ，$n < 4000$ となる． □

このタイプの評価からさらにわかることがある．(2) 式から同じ方法で，

$$\prod_{n<p\leq 2n} p \geq 2^{\frac{1}{30}n} \qquad (n \geq 4000)$$

であることを，また，n と $2n$ の間の領域には少なくとも

$$\log_{2n}\left(2^{\frac{1}{30}n}\right) = \frac{1}{30}\frac{n}{\log_2 n + 1}$$

個の素数が存在することを導くことができる．

これはそれほど悪い評価ではない．というのも，この領域での素数の「本当の」個数は粗っぽく言えば，$n/\log n$ なのである．これは有名な「素数定理」からわかる．素数定理は，極限

$$\lim_{n\to\infty} \frac{\#\{p \leq n : p \text{ は素数 }\}}{n/\log n}$$

が存在して 1 になる，というものである．この有名な結果は最初，アダマールとド・ラ・ヴァレ・プーサンによって 1896 年に証明された．セルバーグとエルデシュは 1948 年に初等的な証明を与えた（複素解析の道具は使わないが，それでも長くて込み入っている）．

素数定理自身については，最終的な言葉は語られていないように見える．たとえば，数学の未解決な大問題の 1 つであるリーマン予想（52 ページ参照）が証明されれば，素数定理の評価に実質的な改良も得られるだろう．しかし，ベルトランの仮説に関してもまた，劇的な改良を期待することもできるだろう．実際，次の問題は未解決である [3, p. 19].

n^2 と $(n+1)^2$ の間に常に素数があるか？

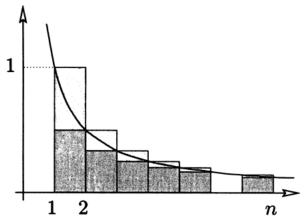
附録：いくつかの評価

積分による評価

和を積分によって評価する，非常に単純だが効果的な方法が存在する（5ページに既出）．調和数

$$H_n = \sum_{k=1}^{n} \frac{1}{k}$$

を評価するには，余白にある図を描き，その図から，$f(t) = \frac{1}{t}$ $(1 \le t \le n)$ のグラフの下の面積と濃い影をつけた長方形の面積とを比較して，



$$H_n - 1 = \sum_{k=2}^{n} \frac{1}{k} < \int_1^n \frac{1}{t}\,dt = \log n$$

を導き，（薄い影の部分を含む）大きな長方形の面積とを比較して

$$H_n - \frac{1}{n} = \sum_{k=1}^{n-1} \frac{1}{k} > \int_1^n \frac{1}{t}\,dt = \log n$$

を導く．これを合わせると，

$$\log n + \frac{1}{n} < H_n < \log n + 1$$

が得られる．とくに，$\lim_{n\to\infty} H_n \to \infty$ であり，H_n の増大のオーダーは $\lim_{n\to\infty} \frac{H_n}{\log n} = 1$ で与えられる．しかし，ずっとよい評価

$$H_n = \log n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + O\left(\frac{1}{n^6}\right)$$

が知られている（[2] を参照）．ここで，$\gamma \approx 0.5772$ は「オイラーの定数」である．

ここで，$O\left(\frac{1}{n^6}\right)$ は，ある定数 c に対して $f(n) \le c\frac{1}{n^6}$ を満たすような関数 $f(n)$ を表わす．

階乗の評価 —— スターリングの公式

同じ方法を

$$\log(n!) = \log 2 + \log 3 + \cdots + \log n = \sum_{k=2}^{n} \log k$$

に適用すると，

$$\log((n-1)!) \;<\; \int_1^n \log t\,dt \;<\; \log(n!)$$

が得られる．この積分は容易に計算され，

$$\int_1^n \log t\,dt \;=\; \Big[t\log t - t\Big]_1^n \;=\; n\log n - n + 1$$

となる．こうして $n!$ の下からの評価

$$n! \;>\; e^{n\log n - n+1} \;=\; e\left(\frac{n}{e}\right)^n$$

と同時に，上からの評価

$$n! \;=\; n\,(n-1)! \;<\; ne^{n\log n-n+1} \;=\; en\left(\frac{n}{e}\right)^n$$

が得られる．ここで，**スターリングの公式**

$$n! \;\sim\; \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

ここで，$f(n)\sim g(n)$ は $\displaystyle\lim_{n\to\infty}\frac{f(n)}{g(n)}=1$ を意味する．

によって与えられるような $n!$ の漸近挙動を得るには，もっと注意深い解析が必要となる．そしてまた，もっと厳密な

$$n! \;=\; \sqrt{2\pi n}\left(\frac{n}{e}\right)^n\left(1+\frac{1}{12n}+\frac{1}{288n^2}-\frac{139}{5140n^3}+O\left(\frac{1}{n^4}\right)\right)$$

のような評価もある．

2 項係数の評価

2 項係数 $\binom{n}{k}$ の，n 集合の k 部分集合[2]の個数としての定義からすぐに，2 項係数の列 $\binom{n}{0},\binom{n}{1},\ldots,\binom{n}{n}$ の

- 和は $\displaystyle\sum_{k=0}^{n}\binom{n}{k}=2^n$ であり，

[2] ［訳註］n 集合 (n-set) は n 個の元からなる集合のことである．集合の元は多くの場合「点」と考えることができるので n 点集合と訳されることも多い．しかし，本書の内容は非常に多岐にわたっており，点とは言いにくいことも多いし，頻出するときは便利なので，n 集合を使うことにした．ただ，n に具体的な数が入ると，たとえば 2 集合は 2 つの集合か 2 つの元からなる集合かを区別し難いが，本書では前者の意味では使わない．

- 対称 $\binom{n}{k} = \binom{n}{n-k}$

であることがわかる．関数等式 $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$ からすぐにわかることだが，あらゆる n に対して，2 項係数 $\binom{n}{k}$ は対称で，一山の列をなす．つまり，真中に向かって増加していくので，真中の 2 項係数が列の中で 1 番大きい．

$$1 = \binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \cdots > \binom{n}{n-1} > \binom{n}{n} = 1$$

$$\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 3 & & 1 & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}$$

パスカルの三角形.

ここで，$\lfloor x \rfloor$ と $\lceil x \rceil$ はそれぞれ，数 x の最も近い整数への切り下げと切り上げである．

上に述べた階乗に対する漸近公式から，2 項係数の大きさに対する非常に厳密な評価を得ることができる．しかし，この本では次の形の，非常に弱く単純な評価が必要なだけである．すべての k に対して $\binom{n}{k} \leq 2^n$ である一方，$n \geq 2$ に対して

$$\binom{n}{\lfloor n/2 \rfloor} \geq \frac{2^n}{n}$$

が成り立ち，等号が成り立つのは $n = 2$ のときだけである．とくに，$n \geq 1$ に対して

$$\binom{2n}{n} \geq \frac{4^n}{2n}$$

が成り立つ．このことは，真中の 2 項係数である $\binom{n}{\lfloor n/2 \rfloor}$ が，その和が 2^n である列 $\binom{n}{0} + \binom{n}{n}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ の中の最大のものであり，列の平均が $\frac{2^n}{n}$ であることから得られる．

一方，2 項係数に対する上からの評価

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \leq \frac{n^k}{k!} \leq \frac{n^k}{2^{k-1}}$$

に注意しておく．これは，n が（k に比べて）大きいとき，列の端の方にある「小さな」2 項係数に対するかなりよい評価になっている．

参考文献

[1] P. エルデシュ：「チェビシェフの定理の証明」(*Beweis eines Satzes von Tschebyschef*), Acta Sci. Math. (Szeged) **5** (1930-32), 194-198.

[2] ロナルド・L・グレアム，ドナルド・E・クヌース，オーレン・パタシュニク：『具体的な数学．計算機科学の基礎』(*Concrete Mathematics. A Foundation for Computer Science*), Addison-Wesley, Reading MA 1989[3].

[3] G. H. ハーディー，E. M. ライト：『数論入門』(*An Introduction to the Theory of Numbers*), fifth edition, Oxford University Press 1979[4].

3 ［訳註］日本語版は，『コンピュータの数学』（有澤誠，安村通晃，萩野達也，石畑清訳，共立出版，1993）．

4 ［訳註］日本語版は，『数論入門 I, II』（示野信一，矢神毅訳，シュプリンガー・フェアラーク東京，2001）．

第3章　2項係数は（ほとんど）決してベキにならない

ベルトランの仮説のエピローグとして，2 項係数に関する美しい結果を述べてみたい．1892 年にシルヴェスターは，ベルトランの仮説を次のように強めたものを示した．

> **$n \geq 2k$ ならば，$n, n-1, \dots, n-k+1$ の数のうち，少なくとも 1 つは k より大きな素因数 p を持つ．**

$n = 2k$ のとき，ちょうどベルトランの仮説になることに注意する．1934 年にエルデシュは，シルヴェスターの結果の短くて初等的な天書の証明を，ベルトランの仮説の彼自身の証明に沿った形で与えている．シルヴェスターの定理を，次の同値な形に言い換えておく．

> **2 項係数**
>
> $$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \qquad (n \geq 2k)$$
>
> **は，常に素因数 $p > k$ を持つ．**

このことを心に留めて，もう 1 つのエルデシュの宝石「どんなときに，$\binom{n}{k}$ は何かのベキ m^ℓ に等しくなるか？」に移ろう．$k = \ell = 2$ に対しては，つまり，方程式 $\binom{n}{2} = m^2$ には無限個の解があることが容易に示される．実際，$\binom{n}{2}$ が平方数なら，$\binom{(2n-1)^2}{2}$ も平方数である．これを見るために，$n(n-1) = 2m^2$ とおく．すると

$$(2n-1)^2((2n-1)^2-1) = (2n-1)^2 4n(n-1) = 2(2m(2n-1))^2$$

となり，それゆえ

$$\binom{(2n-1)^2}{2} = (2m(2n-1))^2$$

となる．$\binom{9}{2} = 6^2$ から始めれば，無限個の解が得られる．次は $\binom{289}{2} = 204^2$ である．しかし，これですべての解が得られるわけではない．たとえば，$\binom{50}{2} = 35^2$ から始めても新しい系列が得られ，$\binom{1682}{2} = 1189^2$ からも得られる．$k=3$ に対しては，$\binom{n}{3} = m^2$ が一意的な解 $n=50$, $m=140$ を持つことが知られている．しかしもうこれで終わりである．$k \geq 4$ に対しては，どんな $\ell \geq 2$ に対しても解は存在しない．これはエルデシュが独創的な議論で証明したことである．

$\binom{50}{3} = 140^2$ は $k=3$, $\ell=2$ のときの唯一の解．

定理．方程式 $\binom{n}{k} = m^\ell$ は，$\ell \geq 2$ と $4 \leq k \leq n-4$ に対しては，整数解を持たない．

■ **証明．** 最初に，$n \geq 2k$ と仮定してよいことに注意する．というのは，$\binom{n}{k} = \binom{n}{n-k}$ だからである．定理が間違っていて，$\binom{n}{k} = m^\ell$ であると仮定する．背理法による証明を，次の4段階に分けて行う．

(1) シルヴェスターの定理により，$\binom{n}{k}$ の k より大きな素因数 p があり，したがって p^ℓ は $n(n-1)\cdots(n-k+1)$ を割り切る．明らかに，この因数 $n-i$ の1つだけが p の倍数になり得るので（$p > k$ だから），$p^\ell \mid n-i$ が得られ[1]，したがって

$$n \;\geq\; p^\ell \;>\; k^\ell \;\geq\; k^2$$

となる．

(2) 分子の任意の因数 $n-j$ を考え，$n-j = a_j m_j^\ell$ の形に書く．ここで，a_j はどんな自明でない ℓ 乗数でも割り切れないとする．**(1)** から，a_j の素因数は k 以下のものしかないことに注意する．次に，$i \neq j$ に対して $a_i \neq a_j$ であることを示したい．逆に，ある $i < j$ に対して $a_i = a_j$ であると仮定する．すると $m_i \geq m_j + 1$ であり，

$$k > (n-i)-(n-j) \;=\; a_j(m_i^\ell - m_j^\ell) \;\geq\; a_j((m_j+1)^\ell - m_j^\ell)$$

---

[1] ［訳註］$a \mid b$ は，a が b を割り切ること，つまり，a が b の約数であることを表わす記号である．

$$> a_j \ell m_j^{\ell-1} \ \geq \ \ell(a_j m_j^{\ell})^{1/2} \ \geq \ \ell(n-k+1)^{1/2}$$
$$\geq \ell(\tfrac{n}{2}+1)^{1/2} \ > \ n^{1/2}$$

となるが，これは上の $n > k^2$ に矛盾する．

(3) 次に，a_i は整数 $1, 2, \ldots, k$ をある順序に並べ換えたものになっていることを証明する（エルデシュによれば，これが証明のポイントである）．すでにすべてが異なっていることを知っているのだから，

$$a_0 a_1 \cdots a_{k-1} \quad \text{が} \quad k! \quad \text{を割る}$$

ことを証明すれば十分である．$n-j = a_j m_j^{\ell}$ を方程式 $\binom{n}{k} = m^{\ell}$ に代入すると，

$$a_0 a_1 \cdots a_{k-1}(m_0 m_1 \cdots m_{k-1})^{\ell} \ = \ k! m^{\ell}$$

となる．$m_0 \cdots m_{k-1}$ と m の公約数を消すと，$\gcd(u, v) = 1$ であるものがあって

$$a_0 a_1 \cdots a_{k-1} u^{\ell} \ = \ k! v^{\ell}$$

となる．残っているのは $v = 1$ を示すことである．もしそうでなければ，v は素因数 p を含む．$\gcd(u, v) = 1$ だから，p は $a_0 a_1 \cdots a_{k-1}$ の素因数でなければならず，それゆえ k 以下になる．ルジャンドルの定理（11 ページ参照）によって，$k!$ が p の $\sum_{i \geq 1} \lfloor \frac{k}{p^i} \rfloor$ 乗を含むことがわかっている．

今度は，$n(n-1) \cdots (n-k+1)$ における p のベキを評価する．i を正の整数とし，$b_1 < b_2 < \cdots < b_s$ を $n, n-1, \ldots, n-k+1$ の中での p^i の倍数とする．すると，$b_s = b_1 + (s-1)p^i$ となるので，

$$(s-1)p^i \ = \ b_s - b_1 \ \leq \ n - (n-k+1) \ = \ k-1$$

となり，これから

$$s \ \leq \ \left\lfloor \frac{k-1}{p^i} \right\rfloor + 1 \ \leq \ \left\lfloor \frac{k}{p^i} \right\rfloor + 1$$

が得られる．だから，各 i に対して，$n, \ldots, n-k+1$ の中での，それゆえ a_j たちの中での p^i の倍数の個数は $\lfloor \frac{k}{p^i} \rfloor + 1$ で抑えられる．この

ことから，第2章のルジャンドルの定理に対して使った理屈によって，$a_0a_1\cdots a_{k-1}$ における p のベキは高々

$$\sum_{i=1}^{\ell-1}\left(\left\lfloor\frac{k}{p^i}\right\rfloor+1\right)$$

となることがわかる．唯一の違いは，今回は和を $i=\ell-1$ までしかとらないことだが，それは a_j が ℓ 乗を含まないからである，

この2つを合わせて数えると，v^ℓ における p のベキは高々

$$\sum_{i=1}^{\ell-1}\left(\left\lfloor\frac{k}{p^i}\right\rfloor+1\right)-\sum_{i\geq 1}\left\lfloor\frac{k}{p^i}\right\rfloor \quad\leq\quad \ell-1$$

となる．v^ℓ は ℓ 乗なのだから，これで矛盾が得られた．

これからすでに，$\ell=2$ の場合は示されたことになっている．実際，$k\geq 4$ だから，a_i のうちの1つは4でなければならないが，a_i は平方を含まない．それでこれからは，$\ell\geq 3$ と仮定しよう．

$$50=2\cdot 5^2$$
$$49=1\cdot 7^2$$
$$48=3\cdot 4^2$$

かつ $5\cdot 7\cdot 4=140$

となっていて，ここまでは，我々の解析が $\binom{50}{3}=140^2$ と一致している．

(4) $k\geq 4$ だから，ある i_1,i_2,i_3 に対して $a_{i_1}=1$, $a_{i_2}=2$, $a_{i_3}=4$, つまり

$$n-i_1=m_1^\ell,\quad n-i_2=2m_2^\ell,\quad n-i_3=4m_3^\ell$$

となっていなければならない．すると，$(n-i_2)^2\neq(n-i_1)(n-i_3)$ となる．もしそうでなければ，$b=n-i_2$, $n-i_1=b-x$, $n-i_3=b+y$ $(0<|x|,|y|<k)$ とおいてみると，

$$b^2=(b-x)(b+y)\quad\text{つまり，}\quad(y-x)b=xy$$

となる．ここで，$x=y$ が不可能なことは明らかである．すると，ステップ(1)から

$$|xy| \;=\; b|y-x| \;\geq\; b \;>\; n-k \;>\; (k-1)^2 \;\geq\; |xy|$$

が得られるが[2]，これは不合理である．

[2]［訳註］3つ目の不等式は，ステップ(1)から，$n-k>k^2-k>k^2-k-(k-1)=(k-1)^2$.

だから，$m_2^2 \neq m_1m_3$ となるので，$m_2^2 > m_1m_3$（もう 1 つの場合も同じようにできる）と仮定して，不等式の最後の鎖に進もう．

$$\begin{aligned} 2(k-1)n > n^2-(n-k+1)^2 &> (n-i_2)^2-(n-i_1)(n-i_3) \\ = 4[m_2^{2\ell}-(m_1m_3)^\ell] &\geq 4[(m_1m_3+1)^\ell-(m_1m_3)^\ell] \\ \geq 4\ell m_1^{\ell-1}m_3^{\ell-1} & \end{aligned}$$

が得られる．$\ell \geq 3$ かつ $n > k^\ell \geq k^3 > 6k$ だから，これにより

$$\begin{aligned} 2(k-1)nm_1m_3 > 4\ell m_1^\ell m_3^\ell &= \ell(n-i_1)(n-i_3) \\ > \ell(n-k+1)^2 &> 3(n-\frac{n}{6})^2 > 2n^2 \end{aligned}$$

となる[3]．ここで，$m_i \leq n^{1/\ell} \leq n^{1/3}$ だから，最終的に

$$kn^{2/3} \geq km_1m_3 > (k-1)m_1m_3 > n$$

が，つまり $k^3 > n$ が得られる．これは（ステップ (1) と）矛盾するので，証明は終わりである． □

参考文献

[1] P. エルデシュ：「シルヴェスターとシューアの定理」(*A theorem of Sylvester and Schur*), J. London Math. Soc. **9** (1934), 282-288.

[2] P. エルデシュ：「ディオファントス方程式について」(*On a diophantine equation*), J. London Math. Soc. **26** (1951), 176-178.

[3] J. J. シルヴェスター：「算術級数について」(*On arithmetical series*), Messenger of Math. **21** (1892), 1-19, 87-120; Collected Mathematical Papers Vol. 4, 1912, 687-731.

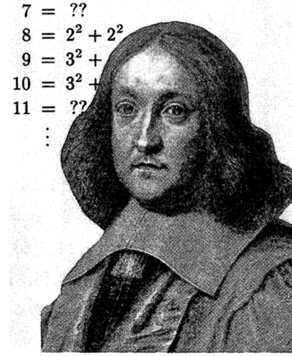
---

[3] [訳註] この不等式の最初と最後の項だけ見て，$2n$ で割ると，次の行の最後の不等式が得られている．

第4章　整数を2つの平方数の和に書く

どんな数が，2つの平方数の和に書くことができるか？

$1 = 1^2 + 0^2$
$2 = 1^2 + 1^2$
$3 = \ ??$
$4 = 2^2 + 0^2$
$5 = 2^2 + 1^2$
$6 = \ ??$
$7 = \ ??$
$8 = 2^2 + 2^2$
$9 = 3^2 +$
$10 = 3^2 +$
$11 = \ ??$
$\vdots$



ピエール・ド・フェルマー

この問題は整数論と同じほど古く，その解はこの分野の古典である．解答の「困難な」部分は，$4m+1$ の形のあらゆる素数が2つの平方数の和であることを知ることである．G. H. ハーディーは，このフェルマーの**2平方の定理**は「まったく正当にも，算術で最も素晴らしいものの1つに格づけされるものである」と書いている．しかしながら，以下に述べる我々の天書の証明の1つは極めて最近のものである．

少し「ウォーミング・アップ」しよう．まず，素数を $p=2$ と，$p=4m+1$ の形のものと，$p=4m+3$ の形のものとに分けて考えよう．あらゆる素数はこの3つのクラスのどれか1つに属す．この時点で，(「ユークリッド流の」方法を使って) $4m+3$ の形の素数が無限にあることに注意してもよい．実際，そのようなものが有限個だったとすれば，p_k をこの形の素数で最大のものにとることができる．

$$N_k \;=\; 2^2 \cdot 3 \cdot 5 \cdots p_k - 1$$

(ここで，$p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ はすべての素数の列を表わす) とおけば，N_k は mod 4 で 3 と合同であり，だから $4m+3$ の形の素因数を持たなければならず，この素因数は p_k よりも大きい —— 矛盾．この章の終わりに，もう1種類の $p=4m+1$ の形の素数も無限にあることを導くことにする．

最初の補題は有名な「相互法則」の特別な場合であって，体 $\mathbb{Z}_p$ の中

で -1 が平方数であるような素数を特徴付けるものである（次ページの箱でこのことを復習する）．

補題 1. 素数 $p = 4m + 1$ に対して，方程式 $s^2 \equiv -1 \pmod{p}$ は 2 つの解 $s \in \{1, 2, \ldots, p-1\}$ を持つ．$p = 2$ のときそのような解は 1 つだが，素数 $p = 4m + 3$ に対しては解はない．

■ **証明.** $p = 2$ のときは $s = 1$ ととれ．奇数 p に対しては，$\{1, 2, \ldots, p-1\}$ 上の同値関係で，各元を $\mathbb{Z}_p$ での加法としての逆元と，さらに乗法としての逆元とを同一視することで生成されるものを考える．こうすると，「一般の」同値類は 4 つの元

$$\{x, -x, \overline{x}, -\overline{x}\}$$

を含んでいる．というのは，そのような 4 集合は，そのすべての元の両方の逆元を含んでいるからである．しかし，この 4 元のいくつかが異なっていなければ，より小さな同値類がある．

- p が奇数のとき，$x \equiv -x$ は起こり得ない．
- $x \equiv \overline{x}$ は $x^2 \equiv 1$ と同値である．これは 2 つの解，つまり $x = 1$, $x = p - 1$ を持つので，大きさ 2 の同値類 $\{1, p-1\}$ になる．
- $x \equiv -\overline{x}$ は $x^2 \equiv -1$ と同値である．この方程式は解を持たないか，2 つの異なる解 $x_0, p - x_0$ を持つかである．あとの場合，同値類は $\{x_0, p - x_0\}$ である．

$p = 11$ に対しては，分割は $\{1, 10\}$, $\{2, 9, 6, 5\}$, $\{3, 8, 4, 7\}$ であり，$p = 13$ に対しては $\{1, 12\}$, $\{2, 11, 7, 6\}$, $\{3, 10, 9, 4\}$, $\{5, 8\}$ である．対 $\{5, 8\}$ は $s^2 \equiv -1 \bmod 13$ の 2 つの解である．

集合 $\{1, 2, \ldots, p-1\}$ は $p-1$ 個の元を持ち，これを，4 つ組み（大きさ 4 の同値類）と，1 つまたは 2 つの対（大きさ 2 の同値類）に分割したことになる．$p-1 = 4m+2$ に対しては，対は 1 つ $\{1, p-1\}$ だけで，残りは 4 つ組みになり，$s^2 \equiv -1 \pmod{p}$ には解はない．$p - 1 = 4m$ に対しては，もう 1 つ対がなければならず，この対が求めていた $s^2 \equiv -1 \pmod{p}$ の 2 つの解である．□

素体

p が素数なら，集合 $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ に,「p を法として」定義された加法と乗法を考えると，有限体になる．以下の簡単な性質はあとで必要になる．

- $x \in \mathbb{Z}_p$, $x \neq 0$ に対して，加法の逆元（通常これを $-x$ と書く）は $p - x \in \{1, 2, \ldots, p-1\}$ によって与えられる．$p > 2$ ならば，x と $-x$ は $\mathbb{Z}_p$ の異なる元である．

- 各 $x \in \mathbb{Z}_p \backslash \{0\}$ には乗法的な逆元 $\overline{x} \in \mathbb{Z}_p \backslash \{0\}$，つまり，$x\overline{x} \equiv 1 \pmod{p}$ を満たすものがある．

  素数の定義から，すべての $x \neq 0$ に対して，写像 $\mathbb{Z}_p \to \mathbb{Z}_p$, $z \mapsto xz$ は単射である．すると，有限集合 $\mathbb{Z}_p \backslash \{0\}$ 上では全射にもなっていなければならないので，各 x に対して，$x\overline{x} \equiv 1 \pmod{p}$ を満たす元 $\overline{x} \neq 0$ が一意的に存在する．

- 平方 $0^2, 1^2, 2^2, \ldots, h^2$ は，$h = \lfloor \frac{p}{2} \rfloor$ に対して，$\mathbb{Z}_p$ の異なる元を定める．
  これは，$x^2 \equiv y^2$, つまり $(x+y)(x-y) \equiv 0$ から $x \equiv y$ または $x \equiv -y$ が得られるからである．$1 + \lfloor \frac{p}{2} \rfloor$ 個の元 $0^2, 1^2, \ldots, h^2$ は $\mathbb{Z}_p$ において**平方数**と呼ばれる．

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_5$ における加法と乗法.

ここで，話は違うが，すべての素数に対して，$x^2 + y^2 \equiv -1 \pmod{p}$ が解を持つことを注意しておく．実際，$\mathbb{Z}_p$ には $\lfloor \frac{p}{2} \rfloor + 1$ 個の異なる平方数 x^2 があり，$-(1+y^2)$ という形をした $\lfloor \frac{p}{2} \rfloor + 1$ 個の異なる数がある．$\mathbb{Z}_p$ には p 個の元しかないから，この 2 つの数の集合は大き過ぎて，交わってしまう．こうして，$x^2 \equiv -(1+y^2) \pmod{p}$ を満たす x と y が存在しなければならない．

補題 2. 2 つの平方数の和になる数 $n = 4m + 3$ はない.

■ **証明.** 偶数の平方数は $(2k)^2 = 4k^2 \equiv 0 \pmod 4$ であり，奇数の平方数は $(2k+1)^2 = 4(k^2+k)+1 \equiv 1 \pmod 4$ を満たす．こうして，任意の 2 つの平方数の和は mod 4 で，$0, 1, 2$ のどれかと合同である． □

このことは，素数 $p = 4m+3$ が「よくない」ことの十分な証拠になっている．そこで，$p = 4m+1$ の形の素数に対する「よい」性質に進もう．主定理への道筋の中で，次は鍵になるステップである．

命題. $p = 4m+1$ **の形のあらゆる素数は 2 つの平方数の和である．つまり，ある自然数** $x, y \in \mathbb{N}$ **を使って，**$p = x^2 + y^2$ **と書くことができる．**

ここで，この結果の 2 つの証明を紹介しよう．ともにエレガントで意外性がある．第 1 の証明の特徴は，「鳩の巣原理」（すでに補題 2 の前で話のついでに使っているが，それ以上は第 21 章を参照のこと）の印象的な応用であり，さらに「p を法とする」議論との間をスマートに行き来することである．このアイデアは，ノルウェーの整数論家アクサル・トゥエに帰される．

$p = 13$, $\lfloor\sqrt{p}\rfloor = 3$ に対して $x', y' \in \{0, 1, 2, 3\}$ を考える．$s = 5$ に対しては，和 $x' - sy' \pmod{13}$ は以下の値をとる．

$x' \backslash y'$	0	1	2	3
0	0	8	3	11
1	1	9	4	12
2	2	10	5	0
3	3	11	6	1

■ **証明.** 整数の対 (x', y') で，$0 \le x', y' \le \sqrt{p}$ を，つまり $x', y' \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}$ を満たすものを考える．そのような対は $(\lfloor\sqrt{p}\rfloor + 1)^2$ 個ある．$x = \sqrt{p}$ に対して評価 $\lfloor x \rfloor + 1 > x$ を使えば，そのような整数の対の個数は p より大きい．こうして，任意の $s \in \mathbb{Z}$ に対して，対 (x', y') によって作られる値 $x' - sy'$ のすべてが，p を法として異なることはあり得ない．つまり，あらゆる s に対し，2 つの異なる対

$$(x', y'),\ (x'', y'') \quad \in \quad \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}^2$$

であって，

$$x' - sy' \quad \equiv \quad x'' - sy'' \pmod p$$

を満たすものがある．そこで差をとると，$x' - x'' \equiv s(y' - y'') \pmod p$ となる．つまり，

$$x = |x' - x''|, \quad y = |y' - y''|$$

とおけば，

$$x \equiv \pm sy \pmod p \quad \text{を満たす対} \quad (x, y) \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}^2$$

が得られる．また，対 (x',y') と (x'',y'') が異なっているので，x と y の両方は 0 になれない．

さて，s を $s^2 \equiv -1 \pmod p$ の解とする．この存在は補題 1 による．すると $x^2 \equiv s^2y^2 \equiv -y^2 \pmod p$ となり，こうして

$$0 < x^2 + y^2 < 2p \text{ と } x^2 + y^2 \equiv 0 \pmod p \text{ を満たす } (x,y) \in \mathbb{Z}^2$$

が作られている．しかし，p は，0 と $2p$ の間の数で p で割り切れる唯一の数である．こうして $x^2 + y^2 = p$ となる．できた！ □

命題の第 2 の証明は，これも明らかに天書の証明だが，1971 年にロジャー・ヒース=ブラウンによって発見され，1984 年に公表された（凝縮された「1 文版」がドン・ザギエによって与えられた[1]）．これはあまりに初等的で，補題 1 を使う必要もない．

ヒース=ブラウンの議論の特徴は 3 つの線形な対合にある．1 つは極めて明らかなもの，2 つ目は隠されたもの，3 つ目は「止めの一撃」を与える自明なものである．思い付きにくい第 2 の対合は，方程式 $4xy+z^2=p$ の整数解の集合のある隠れた構造に対応している．

■ **証明．** 集合

$$S = \{(x,y,z) \in \mathbb{Z}^3 : 4xy + z^2 = p, \quad x > 0, \quad y > 0\}$$

を調べる．これは有限集合である．実際，$x \geq 1$ かつ $y \geq 1$ だから，$y \leq \frac{p}{4}$ かつ $x \leq \frac{p}{4}$ となっている．それゆえ，x と y の可能な値は有限個しかなく，与えられた x と y に対する z の値は高々2 つである．

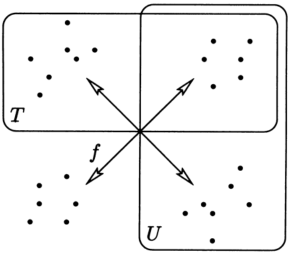
1. 最初の線形な対合は

$$f : S \longrightarrow S, \quad (x,y,z) \longmapsto (y,x,-z)$$

によって与える．つまり,「x と y を交換し，z の符号を変える」とする．これは明らかに，S を自分自身に写す**対合**，つまり 2 度行えば恒等写像になる．また f は固定点を持たない．というのは，$z=0$ から $p=4xy$ が得られるが，それは起こり得ないからである．さらに，f は

$$T = \{(x,y,z) \in S : z > 0\}$$

1 ［訳註］本書の原著初版ではザギエの表現に沿った形での証明の解説が，美しい図版とともに掲載されていた．この第 2 版ではより初等的な形に書き直されている．



に属す解を，$S \backslash T$ に属す解，つまり $z<0$ を満たす解に写す．また，f は $x-y$ と z の符号を変えるので，

$$U \quad = \quad \{(x,y,z) \in S : (x-y)+z>0\}$$

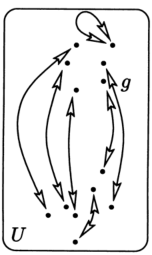
に属す解を，$S \backslash U$ に属す解に写す．このためには，$(x-y)+z=0$ を満たす解がないことを見なければならないが，解なら $p=4xy+z^2=4xy+(x-y)^2=(x+y)^2$ となって，これもあり得ない．

f を調べることから何がわかるか？ 主な観察は，f が集合 T と U をその補集合に写すので，$T \backslash U$ の元と $U \backslash T$ の元を交換することである．つまり，T に属さず U に属す解と，U に属さず T に属す解の数は同じである．それゆえ，**T と U は同じ濃度を持つ．**

2.　次に調べる対合は集合 U 上の対合

$$g : U \longrightarrow U, \quad (x,y,z) \longmapsto (x-y+z, y, 2y-z)$$

である．まずこれが写像としてちゃんと定義されていることを確かめる．$(x,y,z) \in U$ であれば，$x-y+z>0$，$y>0$ かつ $4(x-y+z)y+(2y-z)^2=4xy+z^2$ となるので，$g(x,y,z) \in S$ である．$(x-y+z)-y+(2y-z)=x>0$ だから実際 $g(x,y,z) \in U$ となる．



また，g は対合である．つまり，$g(x,y,z)=(x-y+z,y,2y-z)$ は g によって，$((x-y+z)-y+(2y-z), y, 2y-(2y-z))=(x,y,z)$ に写される．

そして最後に，g は固定点を 1 つ持っている．

$$(x,y,z) \quad = \quad g(x,y,z) \quad = \quad (x-y+z, y, 2y-z)$$

が成り立つのは，ちょうど $y=z$ のときである．しかしそのとき，$p=4xy+y^2=(4x+y)y$ となるが，それは $y=1=z$ かつ $x=\frac{p-1}{4}$ のときしか成り立たない．

しかし，g が U 上の対合で，固定点が 1 つならば，**U の濃度は奇数である．**

3.　3 番目に調べる自明な対合は，T 上の対合

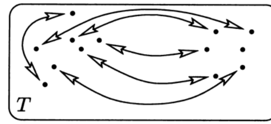
$$h : T \longrightarrow T, \quad (x,y,z) \longmapsto (y,x,z)$$

で，x と y を交換するものである．この写像は明らかにちゃんと定義さ

れた対合である．ここで他の 2 つの対合から得られた知識，つまり，T の濃度と U の濃度は等しくて，奇数であることを組み合わせる．しかし，h が奇数濃度の有限集合上の対合ならば，**固定点がある．** $x = y$ を満たす点 $(x, y, z) \in T$ が存在し，

$$p = 4x^2 + z^2 = (2x)^2 + z^2$$

の解が存在することになる． □



奇数濃度の有限集合上では，あらゆる対合は少なくとも 1 つの固定点を持つ．

この証明は，さらに次のことも示していることに注意する.「$p = 4m+1$ の形のすべての素数に対して，p を $p = x^2 + (2y)^2$ の形に表わす仕方は**奇数**通りである.」(表示は実際には一意的である．[2] を参照のこと.) また，両方の証明とも実際的でないことを注意しておく．10 桁の素数 p に対して，x と y を求めてごらんなさい！ 2 つの平方数の和としてのそのような表示を見つける効果的な方法は，[5] で議論されている．

次の定理はこの章の初めの問題に完全に答えるものである．

定理．自然数 n が 2 つの平方数の和に表わすことができるのは，n の素因数分解における $p = 4m + 3$ の形のあらゆる素因数の指数が偶数であるとき，かつそのときに限る．

■ **証明．** 数 n が 2 つの平方数の和であるとき，つまり，ある $x, y \in \mathbb{N}_0$ に対して $n = x^2 + y^2$ となるとき，**表示可能**であると呼ぼう．定理は以下の 5 つの事実の結果である．

(1) $1 = 1^2 + 0^2$ と $2 = 1^2 + 1^2$ は表示可能である．$p = 4m + 1$ の形のあらゆる素数は表示可能である．

(2) 2 つの表示可能な数 $n_1 = x_1^2 + y_1^2$ と $n_2 = x_2^2 + y_2^2$ の積は表示可能である．つまり，$n_1 n_2 = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2$.

(3) n が表示可能 $n = x^2 + y^2$ であれば，nz^2 も表示可能である．つまり，$nz^2 = (xz)^2 + (yz)^2$.

事実 (1), (2), (3) を合わせると，定理の「のとき」の部分が得られる．

(4) $p = 4m + 3$ が表示可能な数 $n = x^2 + y^2$ を割る素数であれば，p は x と y の双方を割り，だから p^2 は n を割る．実際，$x \not\equiv 0 \pmod p$ であるのなら，$x\overline{x} \equiv 1 \pmod p$ を満たす $\overline{x}$ を見つ

けることができ，方程式 $x^2+y^2 \equiv 0$ に $\overline{x}^2$ を掛けると，$1+y^2\overline{x}^2 = 1+(\overline{x}y)^2 \equiv 0 \pmod p$ が得られる．補題1により，$p=4m+3$ に対して，これは起こり得ない．

(5) n が表示可能で，$p=4m+3$ が n を割るなら，p^2 は n を割り，n/p^2 は表示可能である．このことは (4) から得られ，これで証明は完結する． □

系として，$p=4m+1$ の形の素数が無限個あることもわかる．このために，mod 4 で 1 と合同な数

$$M_k = (3\cdot 5\cdot 7\cdots p_k)^2 + 2^2$$

を考える．そのすべての素因数は p_k より大きく，上の証明の事実 (4) から，$4m+3$ の形をした素因数はない．こうして，M_k は，p_k より大きく，$4m+1$ の形の素因数を持っている．

次の2つの注意で，ここの議論を締めくくることにしよう．

- a と b が互いに素な2つの自然数であれば，$am+b \ (m \in \mathbb{N})$ の形をした素数が無限個ある．— これが有名な（そして難しい）ディリクレの定理である．
- しかし，a を固定して b を変えるとき，同じ割合で素数が現れるということは，$a=4$ に対してさえも，まったく正しくはない．これは一見正しそうにみえるが，$4m+1$ の形の素数より $4m+3$ の形の素数の方が「ずっとたくさん」あるという微妙な傾向が発見されている．この効果は「チェビシェフの偏り」として知られている．ルビンシュタインとサルナク [3] を参照のこと．

参考文献

[1] D. R. ヒース=ブラウン：「フェルマーの2平方定理」(*Fermat's two squares theorem*), Invariant (1984), 2-5.

[2] I. ニーヴン，H.S. ツッカーマン：『数論入門，第3版』(*An Introduction to the Theory of Numbers*), third edition, Wiley 1972.

[3] M. ルビンシュタイン，P. サルナク：「チェビシェフの偏り」(*Chebyshev's bias*), Experimental Mathematics **3** (1994), 173-197.

[4] A. トゥエ：「数論的方法のいくつかのヒント」(*Et par antydninger til en taltheoretisk metode*), Kra. Vidensk. Selsk. Forh. **7** (1902), 57-75[2].

[5] S. ワゴン：「編集者のコーナー：ユークリッドのアルゴリズムがまたやった」(*Editor's corner: The Euclidean algorithm strikes again*), Amer. Math. Monthly **97** (1990), 125-129.

[6] ドン・ザギエ：「あらゆる素数 $p \equiv 1 \pmod 4$ が 2 つの平方数の和であることの 1 文の証明」(*A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares*), Amer. Math. Monthly **97** (1990), 144.

[2] [訳註] "Kra" はクリスティアニア（オスロの古名）の短縮形．ノルウェー語の雑誌．

第5章　あらゆる有限可除環は体である



エルンスト・ヴィット

環は現代の代数学では重要な構造である．環 R が乗法の単位元 1 を持ち，あらゆる 0 でない元が乗法の逆元を持つとき，R は**可除環**と呼ばれる[1]．つまり，R が体であるために足りないのは，乗法の可換性だけである．非可換な可除環の一番よく知られた例と言えば，ハミルトンによって発見された四元数のなす環である[2]．しかし，章題で述べているように，そのような環はすべて，必ず無限になってしまう．もし R が有限ならば，公理のために乗法は可換になってしまうのである．

今では古典となったこの結果は，多くの数学者の想像力を刺激してきた．というのも，ヘルシュタインが言っているように，「それは，ある代数系の元の数とその系での乗法という，2 つの関係しそうもない事柄の予期することのできない関りを示す」ものだからである．

定理．あらゆる有限可除環 R は体である．

この美しい定理は通常マクラガン・ウェダーバーンに帰されているが，多くの人々によって様々の異なるアイデアを使って証明されてきた．ウェダーバーン自身も 1905 年に 3 つの証明を与えているし，もう 1 つの証明が同じ年にレオナード・E・ディクソンによって与えられた．のちにさ

---

[1] ［訳註］斜体と呼ばれることも多い．またさらに，乗法に関して可換なときに体という．この流儀とは別に，可除環＝斜体を単に体と言い，上の意味での体を可換体という流儀もある．2 つの流儀を混同しなければ，どちらを使ってもよいが，日本では後者の流儀の方が多数派であり，その流儀では，定理は「有限体は可換である」ということになる．

[2] ［訳註］上の中で述べたように，日本では四元数体と呼ぶことが多い．

らに多くの証明が，エミール・アルティン，ハンス・ツァッセンハウス，ニコラ・ブルバキ，その他多くの人によって与えられた．1つの証明が単純さとエレガントさによって際だっている．それは1931年にエルンスト・ヴィットによって発見されたもので，栄光のゴールに向かって2つの初等的なアイデアを組み合わせたものである．

■ **証明．** 最初の要素は線形代数のものである．任意の元 $s \in R$ に対して，s と可換な元の集合 $\{x \in R : xs = sx\}$ を C_s とし，C_s を s の**交換子環**と言う．明らかに，C_s は 0 と 1 を含み，R の部分可除環である．**中心** Z は R のすべての元と可換な元の集合であり，$Z = \bigcap_{s \in R} C_s$ となる．とくに，Z のすべての元は交換し，0 と 1 が Z に属すので，Z は**有限体**である．$|Z| = q$ とおく．

R と C_s を体 Z 上のベクトル空間とみなすことができ，Z 上のベクトル空間 R の次元 n に対して，$|R| = q^n$ であること，また同じように適当な整数 $n_s \geq 1$ に対して $|C_s| = q^{n_s}$ であることを導くことができる．

ここで，R が体でないと仮定しよう．つまり，ある $s \in R$ に対して交換子環 C_s が R 全体でないこと，または同じことだが，$n_s < n$ であるとする．

集合 $R^* = R\backslash\{0\}$ 上に，関係

$$r' \sim r \quad \Longleftrightarrow \quad r' = x^{-1}rx \quad (\text{ある } x \in R^* \text{ に対して})$$

を考える．この $\sim$ が同値関係であることは容易に確かめられる．

$$A_s \;=\; \{x^{-1}sx : x \in R^*\}$$

を s を含む同値類とする．$|A_s| = 1$ であるのはちょうど s が中心 Z に属すときであることを注意しておく．すると仮定により，$|A_s| \geq 2$ であるような類 A_s が存在する．そこで，$s \in R^*$ に対して，R^* から A_s の上への写像 $f_s : x \longmapsto x^{-1}sx$ を考えると，

$$\begin{aligned} x^{-1}sx = y^{-1}sy &\Longleftrightarrow (yx^{-1})s = s(yx^{-1}) \\ &\Longleftrightarrow yx^{-1} \in C_s^* \quad \Longleftrightarrow \quad y \in C_s^* x \end{aligned}$$

であることがわかる．ここで，$C_s^* x = \{zx : z \in C_s^*\}$ の大きさは $|C_s^*|$ である．それゆえ，どんな元 $x^{-1}sx$ も，R^* のちょうど $|C_s^*| = q^{n_s} - 1$ 個の元の，写像 f_s による像になっており，$|R^*| = |A_s|\,|C_s^*|$ が導かれ

る．とくに，すべての s に対して

$$\frac{|R^*|}{|C_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |A_s| \quad \text{は整数}$$

であることに注意する．同値類による R^* の分割はわかっている．そこで，中心の元を集めて Z^* とし，2 つ以上の元を含む同値類を $A_1, \ldots, A_t$ と書く．仮定により，$t \geq 1$ である．$|R^*| = |Z^*| + \sum_{i=1}^{t} |A_i|$ だから，いわゆる**類公式**

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1} \tag{1}$$

が証明されたことになる．ここで，すべての i に対して $1 < \frac{q^n-1}{q^{n_i}-1} \in \mathbb{N}$ である．

(1) が得られ，抽象代数から離れて，自然数の話になっている．次に，$q^{n_i} - 1 \,|\, q^n - 1$ から $n_i \,|\, n$ が導かれることを示す．実際，$n = an_i + r$, $0 \leq r < n_i$ と書けば，$q^{n_i} - 1 \,|\, q^{an_i + r} - 1$ から

$$q^{n_i} - 1 \,|\, (q^{an_i + r} - 1) - (q^{n_i} - 1) = q^{n_i}(q^{(a-1)n_i + r} - 1)$$

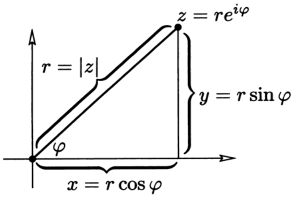
が得られる．q^{n_i} と $q^{n_i} - 1$ は互いに素だから，$q^{n_i} - 1 \,|\, q^{(a-1)n_i + r} - 1$ である．これを続けると，$q^{n_i} - 1 \,|\, q^r - 1$ $(0 \leq r < n_i)$ が得られるが，これが成り立つのは $r = 0$ のとき，つまり，$n_i \,|\, n$ のときだけである．まとめると，すべての i に対して

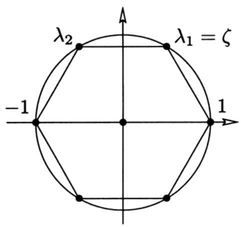
$$n_i \,|\, n \tag{2}$$

となる．

今度は第 2 の要素である複素数 $\mathbb{C}$ の番である．多項式 $x^n - 1$ を考える．$\mathbb{C}$ におけるその根を 1 の n **乗根**と言う．これらの根 λ は，$\lambda^n = 1$ だから，すべて $|\lambda| = 1$ を満たし，したがって複素平面の単位円周上にある．実際，きちんと書けば，$\lambda_k = e^{\frac{2k\pi i}{n}} = \cos(2k\pi/n) + i\sin(2k\pi/n)$, $0 \leq k \leq n-1$ という数である（次ページの箱を参照）．根 λ のうちには，$d < n$ に対して $\lambda^d = 1$ を満たすものがある．たとえば，根 $\lambda = -1$ は $\lambda^2 = 1$ を満たす．根 λ に対して，$\lambda^d = 1$ を満たす最小の正の指数を d とする．つまり，d は 1 のベキ根の作る群における λ の位数である．すると，ラグランジュの定理により，$d \,|\, n$ である（「群のあらゆる

元の位数は群の位数を割る」—— 第1章の余白の箱を参照のこと）．たとえば $\lambda_1 = e^{\frac{2\pi i}{n}}$ のように，位数 n の根があることに注意する．





$n = 6$ のときの1のベキ根．

1のベキ根

どんな複素数 $z = x + iy$ も「極」形式

$$z \;=\; re^{i\varphi} \;=\; r(\cos\varphi + i\sin\varphi)$$

に書くことができる．ここで，$r = |z| = \sqrt{x^2 + y^2}$ は原点から z までの距離で，φ は正の x 軸から測った角である．したがって，1の n 乗根は

$$\lambda_k = e^{\frac{2k\pi i}{n}} = \cos(2k\pi/n) + i\sin(2k\pi/n), \qquad 0 \le k \le n-1$$

という形をしている．すべての k に対して

$$\lambda_k^n = e^{2k\pi i} = \cos(2k\pi) + i\sin(2k\pi) = 1$$

となるからである．これらの根は，単位円に内接する正 n 角形から幾何的に得られる．$\zeta = e^{\frac{2\pi i}{n}}$ とすると，すべての k に対して $\lambda_k = \zeta^k$ となることに注意する．こうして，1の n 乗根は，位数 n の巡回群 $\{\zeta, \zeta^2, \ldots, \zeta^{n-1}, \zeta^n = 1\}$ をなす．

さて，位数 d の根をすべて集め，

$$\phi_d(x) \;=\; \prod_{\lambda:\ \text{位数 } d} (x - \lambda)$$

とおく．$\phi_d(x)$ の定義が n に関係しないことに注意する．あらゆる根はある位数 d を持つから，

$$x^n - 1 \;=\; \prod_{d\,|\,n} \phi_d(x) \tag{3}$$

となる．このとき，「多項式 $\phi_n(x)$ の**係数は整数**（つまり，すべての n に対して，$\phi_n(x) \in \mathbb{Z}[x]$）であり，さらに，定数項は1か -1 である」

ということが鍵となる．

この主張を注意して確かめよう．$n=1$ のときは 1 だけが根であり，$\phi_1(x)=x-1$ となる．そこで帰納法によって進めるとして，すべての $d<n$ に対して $\phi_d(x)\in\mathbb{Z}[x]$ であり，$\phi_d(x)$ の定数項が 1 か -1 であると仮定する．(3) によって

$$x^n-1 \;=\; p(x)\,\phi_n(x) \tag{4}$$

となる．ここで，$p(x)=\sum_{i=0}^{\ell}p_ix^i$，$\phi_n(x)=\sum_{j=0}^{n-\ell}a_jx^j$ であり，また $p_0=1$ または $p_0=-1$ である．

$-1=p_0a_0$ だから，$a_0\in\{1,-1\}$ である．すでに $a_0,a_1,\ldots,a_{k-1}\in\mathbb{Z}$ であることがわかっていると仮定する．(4) の両辺の x^k の係数を計算すると，

$$\sum_{i=0}^{k}p_ia_{k-i} \;=\; \sum_{i=1}^{k}p_ia_{k-i}+p_0a_k \;\in\; \mathbb{Z}$$

となる．仮定により，すべての $a_0,\ldots,a_{k-1}$（とすべての p_i）は $\mathbb{Z}$ に属している．こうして，p_0a_k は，それゆえ a_k もまた整数でなければならない．なぜなら，p_0 は 1 か -1 だからである．

止めの一撃を出すときがきた．$n_i\,|\,n$ を (1) に出てくる数の 1 つとすると，

$$x^n-1 \;=\; \prod_{d\,|\,n}\phi_d(x) \;=\; (x^{n_i}-1)\phi_n(x)\prod_{d\,|\,n,\,d\nmid n_i,\,d\neq n}\phi_d(x)$$

となる．$\mathbb{Z}$ において，

$$\phi_n(q)\mid q^n-1 \qquad \text{かつ} \qquad \phi_n(q)\;\Big|\;\frac{q^n-1}{q^{n_i}-1} \tag{5}$$

という，割り算ができるという関係が成り立つことになる．すべての i に対して (5) が成り立つので，類公式 (1) から，

$$\phi_n(q)\,|\,q-1$$

となるのだが，これはあり得ない．なぜか？ $\phi_n(x)=\prod(x-\lambda)$ で，λ は位数 n の x^n-1 のすべての根を動いている．$\widetilde{\lambda}=a+ib$ をその根の

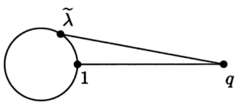
1 つとする．($R \neq Z$ なので) $n > 1$ だから，$\widetilde{\lambda} \neq 1$ となり，その実部 a は 1 より小さい．ここで，$|\widetilde{\lambda}|^2 = a^2 + b^2 = 1$ であり，それゆえ

$$\begin{aligned} |q - \widetilde{\lambda}|^2 = |q - a - ib|^2 &= (q-a)^2 + b^2 \\ = q^2 - 2aq + a^2 + b^2 &= q^2 - 2aq + 1 \\ > q^2 - 2q + 1 & \qquad (a < 1 \text{ だから}) \\ = (q-1)^2 & \end{aligned}$$

となり，だから，位数 n のすべての根に対して，$|q - \widetilde{\lambda}| > q - 1$ となる．これから

$$|\phi_n(q)| \;=\; \prod_{\lambda} |q - \lambda| > q - 1$$

となるが，このことは $\phi_n(q)$ が $q-1$ の約数になれないことを意味しており，矛盾となる．これで証明が終わる．□



$|q - \widetilde{\lambda}| > |q - 1|$.

参考文献

[1] L.E. ディクソン：「有限代数について」(*On finite algebras*), Nachrichten der Akad. Wissenschaften Göttingen Math.-Phys. Klasse (1905), 1-36; Collected Mathematical Papers Vol. III, Chelsea Publ. Comp, The Bronx, NY 1975, 539-574.

[2] J. H. M. ウェダーバーン：「有限代数についての定理」(*A theorem on finite algebras*), Trans. Amer. Math. Soc. **6** (1905), 349-352.

[3] E. ヴィット：「可換な有限斜体について」(*Über die Kommutativität endlicher Schiefkörper*), Abh. Math. Sem. Univ. Hamburg **8** (1931), 413.

第6章　無理数いろいろ

「π は無理数である.」


シャルル・エルミート

このことはすでに，アリストテレスによって予想されていた．そのときは，円の直径と周は通約可能でないという形の主張であった．この基本的事実の最初の証明は，1766年にヨハン・ハインリッヒ・ランベルトによって与えられた．我々の天書の証明は1947年のイヴァン・ニーヴンによるもので，初等的な解析しか必要としないきわめてエレガントな1ページの証明である．そのアイデアは強力で，それからかなりのことが導かれる．たとえば，それぞれ岩本とコクスマによって示されたように，

- π^2 は無理数であり（これはより強い結果！），
- $r \neq 0$ が有理数のとき，e^r は無理数である

が成り立つ．

しかし，ニーヴンの方法にはルーツと先行する仕事がある．それは，1873年のシャルル・エルミートによる古典的な論文にまで遡ることができる．その論文は，e が超越数，つまり，e が有理数を係数とする多項式の零点にはならないことを初めて確立したものである．

$e = \sum_{k\geq 0} \frac{1}{k!}$ が無理数であることを見るのは容易である．実際，$e = \frac{a}{b}$（$a, b > 0$ を整数として）とすると，$n \geq b$ に対して

$$e = 1 + \tfrac{1}{1} + \tfrac{1}{2} + \tfrac{1}{6} + \tfrac{1}{24} + \cdots$$
$$= 2.718281828\cdots$$

$$N \;=\; n!\Big(e - \sum_{k=0}^{n} \frac{1}{k!}\Big)$$

は整数になる．というのは，$n!e$ と（$0 \le k \le n$ に対して）$\frac{n!}{k!}$ が整数であるからである．しかし，この整数はまた

$$N = \sum_{k \ge n+1} \frac{n!}{k!} = \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots$$

と書くことができる．すると，N を幾何級数（等比級数）と比較することができ，

$$0 < N < \frac{1}{n+1} + \frac{1}{(n+1)^2} + \cdots = \frac{1}{n}$$

となる．N は整数だから，これは起こり得ない．

しかしこのトリックでは，(より強い主張の) e^2 が無理数であることを示すことにも使えない．このため，ここでは，本質的にはシャルル・エルミートによる，別の方法を使う．その方法の鍵は次の簡単な補題である．

補題． **ある $n \ge 1$ を固定し，**

$$f(x) = \frac{x^n(1-x)^n}{n!}$$

とおく．

(i) **関数 $f(x)$ は $f(x) = \frac{1}{n!}\sum_{i=n}^{2n} c_i x^i$ という形の多項式で，係数 c_i は整数である．**

(ii) **$0 < x < 1$ に対して，$0 < f(x) < \frac{1}{n!}$ である．**

(iii) **すべての $k \ge 0$ に対して，微係数 $f^{(k)}(0)$ と $f^{(k)}(1)$ は整数である．**

■ **証明．** (i) と (ii) は明らかである．

(iii) については，(i) によって，k 次の微係数 $f^{(k)}$ は，$n \le k \le 2n$ でない限り，$x = 0$ で 0 であり，またその範囲では $f^{(k)}(0) = \frac{k!}{n!}c_k$ は整数である．$f(x) = f(1-x)$ から，すべての x に対して，$f^{(k)}(x) = (-1)^k f^{(k)}(1-x)$ であり，それゆえ，$f^{(k)}(1) = (-1)^k f^{(k)}(0)$ となって，整数になる．□

定理 1. **あらゆる $r \in \mathbb{Q}\backslash\{0\}$ に対して，e^r は無理数である．**

■ **証明．** 正の整数 s に対して e^s が有理数になり得ないことを示せばよい（もし $e^{\frac{s}{t}}$ が有理数なら $\left(e^{\frac{s}{t}}\right)^t = e^s$ も有理数になる）．ある整数 $a, b > 0$ に対して $e^s = \frac{a}{b}$ であると仮定し，n を，$n! > as^{2n+1}$ となるほど十分大きくとる．$f(x)$ を補題の関数として，

「十分大きい」n を具体的に得るには，$n! > e(\frac{n}{e})^n$ という評価を使う．

$$F(x) = s^{2n}f(x) - s^{2n-1}f'(x) + s^{2n-2}f''(x) \mp \cdots + f^{(2n)}(x)$$

とおく．$F(x)$ は無限和の形

$$F(x) = s^{2n}f(x) - s^{2n-1}f'(x) + s^{2n-2}f''(x) \mp \cdots$$

に書いてもよい．$k > 2n$ に対しては，高階の微係数 $f^{(k)}(x)$ は 0 になるからである．このことから，多項式 $F(x)$ は恒等式

$$F'(x) \ = \ -s\,F(x) + s^{2n+1}f(x)$$

を満たす．微分すると，

$$\frac{d}{dx}\left[e^{sx}F(x)\right] \ = \ se^{sx}F(x) + e^{sx}F'(x) \ = \ s^{2n+1}e^{sx}f(x)$$

が得られ，それゆえ

$$N \ = \ b\int_0^1 s^{2n+1}e^{sx}f(x)dx \ = \ b\left[e^{sx}F(x)\right]_0^1 \ = \ aF(1) - bF(0)$$

となる．補題の (iii) から $F(0)$ と $F(1)$ が整数なので，この N は整数になる．補題の (ii) から N の大きさを上と下から評価することができて，

$$0 \ < \ N \ = \ b\int_0^1 s^{2n+1}e^{sx}f(x)dx \ < \ bs^{2n+1}e^s\frac{1}{n!} \ = \ \frac{as^{2n+1}}{n!} \ < \ 1$$

が得られるが，これでは N は整数にはなれない．矛盾である． □

このトリックはとてもうまくいったので，もう 1 回使ってみよう．

定理 2. **π^2 は無理数である．**

■ **証明．** ある整数 $a, b > 0$ に対して，$\pi^2 = \frac{a}{b}$ と仮定する．多項式

$$F(x) \ = \ b^n\Big(\pi^{2n}f(x) - \pi^{2n-2}f^{(2)}(x) + \pi^{2n-4}f^{(4)}(x) \mp \cdots\Big)$$

π は有理数ではないが，有理数による「よい近似」がある．そのいくつかは古代から知られている．

$$\frac{22}{7} = 3.142857142857\cdots$$
$$\frac{355}{113} = 3.141592920353\cdots$$
$$\frac{104348}{33215} = 3.141592653921\cdots$$
$$\pi = 3.141592653589\cdots$$

は，$F''(x) = -\pi^2 F(x) + b^n \pi^{2n+2} f(x)$ を満たす．

補題の (iii) から，$F(0)$ と $F(1)$ は整数である．微分すると．

$$\begin{aligned}\frac{d}{dx}\left[F'(x)\sin\pi x - \pi F(x)\cos\pi x\right] &= \left(F''(x) + \pi^2 F(x)\right)\sin\pi x \\ &= b^n \pi^{2n+2} f(x)\sin\pi x \\ &= \pi^2 a^n f(x)\sin\pi x\end{aligned}$$

となり，

$$\begin{aligned}N = \pi\int_0^1 a^n f(x)\sin\pi x\,dx &= \left[\frac{1}{\pi}F'(x)\sin\pi x - F(x)\cos\pi x\right]_0^1 \\ &= F(0) + F(1)\end{aligned}$$

は整数となる．さらに，(境界を除いて) 正の関数の積分として定義されているので，N は正である．しかし，十分大きく n を選んで，$\frac{\pi a^n}{n!} < 1$ となるようにすると，補題の (ii) から

$$0 \ < \ N \ = \ \pi\int_0^1 a^n f(x)\sin\pi x\,dx \ < \ \frac{\pi a^n}{n!} \ < \ 1$$

が得られる．これは矛盾である．　□

この最後の定理とオイラーによる次の古典的な結果を合わせると，リーマンのゼータ関数（52 ページの附録参照）の値

$$\zeta(2) \ = \ \sum_{n\geq 1}\frac{1}{n^2}$$

が無理数であることが示される．

定理 3. $\displaystyle\sum_{n\geq 1}\frac{1}{n^2} \ = \ \frac{\pi^2}{6}.$

■ **証明.** 以下の証明は，1956 年に刊行されたウィリアム・J・ルヴェクの数論の教科書に演習問題として出ているもので，のちにトム・アポストルによって再発見された．証明は，2 重積分

$$I \ = \ \int_0^1\int_0^1 \frac{1}{1-xy}\,dx\,dy$$

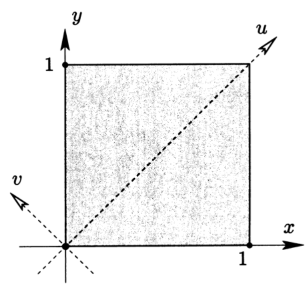
の値を2通りの方法で求めることからなっている．1つ目は，$\frac{1}{1-xy}$ を等比級数に展開し，各項を積に分解して積分する．これは難しくない．つまり，

$$I = \int_0^1\int_0^1 \sum_{n\ge 0}(xy)^n\,dx\,dy \;=\; \sum_{n\ge 0}\int_0^1\int_0^1 x^n y^n\,dx\,dy$$
$$= \sum_{n\ge 0}\left(\int_0^1 x^n dx\right)\left(\int_0^1 y^n dy\right) \;=\; \sum_{n\ge 0}\frac{1}{n+1}\,\frac{1}{n+1}$$
$$= \sum_{n\ge 0}\frac{1}{(n+1)^2} \;=\; \sum_{n\ge 1}\frac{1}{n^2} \;=\; \zeta(2)$$

とする．この計算で，($x = y = 1$ に極を持つ関数の) 2重積分が有限であることもわかる．また計算は容易で，逆向きにも一本道であり，$\zeta(2)$ の値を求めようとすれば2重積分 I に導かれることに注意する．

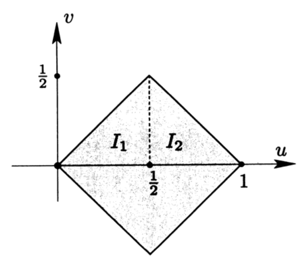
I の2番目の計算法は座標変換をすることである．

$$u = \frac{y+x}{2},\quad v = \frac{y-x}{2}$$



によって与えられる新しい座標では，積分領域は，辺の長さが $\frac{1}{2}\sqrt{2}$ の正方形になる．これは，元の領域から，まず 45° の回転をし，それから長さを $\sqrt{2}$ で割って縮小して得られる．$x = u - v$ と $y = u + v$ を代入すると，

$$\frac{1}{1-xy} \;=\; \frac{1}{1-u^2+v^2}$$



となる．積分を変換するには，この座標変換が面積を2分の1にする（この2は変換のヤコビ行列式による．次ページの箱を参照）という事実を補正するために，$dxdy$ を $2dudv$ に取り換えねばならない．新しい積分領域と被積分関数は u 軸に関して対称だから，上半分の領域での積分の2倍を計算すればよく（ここでもう一度，2という因子がでてくる！），それもきわめて自然に2つの部分に分かれて，

$$I \;=\; 4\int_0^{1/2}\left(\int_0^{u}\frac{dv}{1-u^2+v^2}\right)du \;+\; 4\int_{1/2}^{1}\left(\int_0^{1-u}\frac{dv}{1-u^2+v^2}\right)du$$

> **置換公式**
>
> **2 重積分**
>
> $$I = \int_S f(x,y)\,dx\ dy$$
>
> **を計算するのに,**
>
> $$x = x(u,v) \quad y = y(u,v)$$
>
> **という変数の代入を行ってもよいのは,$(u,v) \in T$ から $(x,y) \in S$ への対応が全単射で連続微分可能なときである.そのとき,I は**
>
> $$\int_T f(x(u,v), y(u,v)) \left|\frac{d(x,y)}{d(u,v)}\right| dudv$$
>
> **に等しい.ただし,$\frac{d(x,y)}{d(u,v)}$ はヤコビ行列式**
>
> $$\frac{d(x,y)}{d(u,v)} = \det\begin{pmatrix} \frac{dx}{du} & \frac{dx}{dv} \\ \frac{dy}{du} & \frac{dy}{dv} \end{pmatrix}$$
>
> **である.**

となる.$\int \frac{dx}{a^2+x^2} = \frac{1}{a}\arctan\frac{x}{a} + C$ を使うと,これは

$$\begin{aligned} I &= 4\int_0^{1/2} \frac{1}{\sqrt{1-u^2}} \arctan\left(\frac{u}{\sqrt{1-u^2}}\right) du \\ &\quad + 4\int_{1/2}^{1} \frac{1}{\sqrt{1-u^2}} \arctan\left(\frac{1-u}{\sqrt{1-u^2}}\right) du \end{aligned}$$

となる.しかしこれらの項は簡単にすることができる.結局のところ,arctan の値は,$0 \le \theta < \pi/2$ の範囲の角 θ である.$u = \sin\theta$ ならば,$\sqrt{1-u^2} = \cos\theta$ であり,それゆえ $\frac{u}{\sqrt{1-u^2}} = \tan\theta$ となる.同じように,$u = \cos\theta$ ならば,$1-u = 1-\cos\theta = 2\sin^2\frac{\theta}{2}$ で,$\sqrt{1-u^2} = \sin\theta = 2\cos\frac{\theta}{2}\sin\frac{\theta}{2}$ であり,それゆえ $\frac{1-u}{\sqrt{1-u^2}} = \tan\frac{\theta}{2}$ となる.これは一石二鳥である.計算しなければならない積分は

$$I = 4\int_0^{1/2} \frac{\arcsin u}{\sqrt{1-u^2}} du + 4\int_{1/2}^{1} \frac{\frac{1}{2}\arccos u}{\sqrt{1-u^2}} du$$

となる.この形から,仕事を済ますことのできる置換を思いつく.つまり,最初の積分については,$u = \sin\theta$ とおくと,$du = \cos\theta d\theta$ となり,区間 $0 \le u \le \frac{1}{2}$ は $0 \le \theta \le \pi/6$ に対応する.第2の積分については,$u = \cos\theta$ とおくと,$du = -\sin\theta d\theta$ となり,区間 $\frac{1}{2} \le u \le 1$ は $\pi/3 \le \theta \le 0$ に対応する.こうして,

$$\begin{aligned} I &= 4\int_0^{\pi/6} \frac{\theta}{\cos\theta} d\theta + 2\int_0^{\pi/3} \frac{\theta}{\sqrt{1-u^2}} du \\ &= 4\left[\frac{1}{2}\theta^2\right]_0^{\pi/6} + 2\left[\frac{1}{2}\theta^2\right]_0^{\pi/3} \\ &= 2\,\frac{\pi^2}{36} + \frac{\pi^2}{9} = \frac{\pi^2}{6} \end{aligned}$$

が得られる. □

アポストルの証明は,比較的簡単な座標変換を使って,積分から $\zeta(2)$

の値を取り出したものである．全く自明なものでない座標変換を使って完全に自明な積分を導くという，このような証明法の創意に満ちた例が，のちにボイカーズ，カラビ，コルクによって発見された．その公式の出発点は，和 $\sum_{n\geq 1}\frac{1}{n^2}$ を，偶数の項と奇数の項に分けることである．明らかに，偶数の項 $\frac{1}{2^2}+\frac{1}{4^2}+\frac{1}{6^2}+\cdots=\sum_{k\geq 1}\frac{1}{(2k)^2}$ は $\frac{1}{4}\zeta(2)$ となるので，奇数の項 $\frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\cdots=\sum_{k\geq 1}\frac{1}{(2k+1)^2}$ は全体の和 $\zeta(2)$ の 4 分の 3 になる．こうして，定理 3 は次の定理と同値になる．

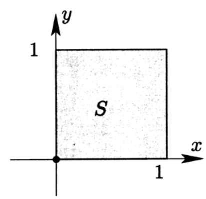
定理 3′. $$\sum_{k\geq 0}\frac{1}{(2k+1)^2} \;=\; \frac{\pi^2}{8}.$$

■ **証明.** 上と同じように，これをたとえば

$$J \;=\; \int_0^1\!\!\int_0^1 \frac{1}{1-x^2y^2}\,dx\,dy \;=\; \sum_{k\geq 0}\frac{1}{(2k+1)^2}$$

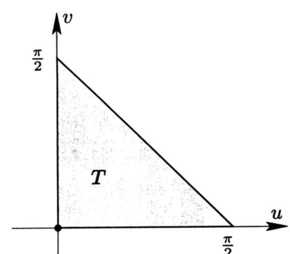
のように 2 重積分で表わすことができる．だからこの積分 J を計算しなければならない．そして，このために，ボイカーズ，カラビ，コルクは

$$u=\arccos\sqrt{\frac{1-x^2}{1-x^2y^2}},\quad v=\arccos\sqrt{\frac{1-y^2}{1-x^2y^2}}$$



という，魔法のような新しい座標を提案した．この 2 重積分を計算するために，積分領域の境界を無視して，$0<x<1$, $0<y<1$ という範囲の x, y を考えることにしてよい．すると，u, v は，三角形 $u>0, v>0, u+v<\pi/2$ の中を動く．この座標変換は，明示的に逆を求めることができ，

$$x=\frac{\sin u}{\cos v},\quad y=\frac{\sin v}{\cos u}$$



という置換をすることになる．この式によって，単位正方形の内部と三角形の内部の間に全単射が定まることを確かめることは易しい．

さて，この座標変換の計算をしなければならないが，これも魔法のように

$$\det\begin{pmatrix}\frac{\cos u}{\cos v} & \frac{\sin u\ \sin v}{\cos^2 v}\\ \frac{\sin u\ \sin v}{\cos^2 u} & \frac{\cos v}{\cos u}\end{pmatrix}=1-\frac{\sin^2 u\ \sin^2 v}{\cos^2 u\cos^2 v}=1-x^2y^2$$

となってしまう．しかし，このことは，計算したかった積分が

$$J = \int_0^{\pi/2}\int_0^{\pi/2-u} 1\,du\,dv$$

に変換されることを意味していて，この積分はまさに三角形 T の面積 $\frac{1}{2}(\frac{\pi}{2})^2 = \frac{\pi^2}{8}$ になる． □

美しい！ その上，すべての $k \geq 1$ に対し，同じ証明法が，$2k$ 次元の積分による $\zeta(2k)$ の計算に拡張できる．ボイカーズ，カラビ，コルクの原論文 [3] と第 19 章を引用しておく．第 19 章では，ヘルグロッツのトリックとオイラーの元のアプローチ[1]を使って別の方法でこれを行っている．

ここで我々は，$\sum_{n\geq 1}\frac{1}{n^2} = \frac{\pi^2}{6}$ のまったく別の証明を述べたくなる誘惑に抵抗することができない．それはまったく初等的で，その上，$\sum_{n=1}^{m}\frac{1}{n^2}$ の $\frac{\pi^2}{6}$ への収束の速さの評価も与えてくれる．その出所についてはあまりはっきりしていない．ジョン・ショウルズによれば，「1960 年代後半に私がイギリスのケンブリッジ大学の学部学生だったときには，この証明は共通の知識だった」のである．この証明は，ケンブリッジ学部生数学同好会（アルキメデスたち）の雑誌『ユリイカ (*Eureka*)』の 1982 年の号 [11] に載ったもので，そこではジョン・ショウルズに帰されている．しかしショウルズが書いていることによれば，「証明は，少なくとも概略（自分で細かいところは補えるようなものだった）はピーター・スウィナートン=ダイアーから聞いたと思うのだが，彼もまた誰か別の人から聞いたと言うだろうと思う」ということである．

しかしながら，この数学の宝石が繰り返し再発見されてきたことと，しばしばわかるように，これもまた 1967 年の A. M. ヤグロムと I. M. ヤグロムの著書（1954 年刊のロシア語原著からの翻訳）にも出ているし，またフィン・ホーム（1970 年）やヨアニス・パパディミトリュ（1973 年）の論文にも現れている．そしてもちろん，基本的なアイデアや恒等式はオイラーにまで遡ることができる．

---

1 ［訳註］ベキ和と基本対称式との関係を使ったオイラーの原証明については，たとえばハイラー–ワナー著『解析教程　上』（シュプリンガー・フェアラーク東京，1997）の I.5 節の演習問題 5.2 参照．

■ **証明.** 第1段階は，コタンジェント関数（の平方）の値の間の顕著な関係を示すことである．つまり，すべての $m \geq 1$ に対して，

$$\cot^2\left(\tfrac{\pi}{2m+1}\right) + \cot^2\left(\tfrac{2\pi}{2m+1}\right) + \cdots + \cot^2\left(\tfrac{m\pi}{2m+1}\right) \;=\; \frac{2m(2m-1)}{6} \qquad (1)$$

が成り立つ．これを示すために，関係式

$$\cos nx + i \sin nx \;=\; (\cos x + i \sin x)^n$$

から始める．虚部をとると，

$$\sin nx \;=\; \binom{n}{1} \sin x \cos^{n-1} x - \binom{n}{3} \sin^3 x \cos^{n-3} x \pm \cdots \qquad (2)$$

となる．ここで $n = 2m+1$ とおき，x としては m 個の異なる値 $x = \frac{r\pi}{2m+1}$ $(r = 1, 2, \ldots, m)$ を考えよう．これらの値に対しては $nx = r\pi$ となり，$\sin nx = 0$ となる．一方で，$0 < x < \frac{\pi}{2}$ だから，$\sin x$ は m 個の異なる正の値をとることになる．

とくに，(2) を $\sin^n x$ で割ることができる．すると

$$0 = \binom{n}{1} \cot^{n-1} x - \binom{n}{3} \cot^{n-3} x \pm \cdots$$

つまり，

$$0 = \binom{2m+1}{1} \cot^{2m} x - \binom{2m+1}{3} \cot^{2m-2} x \pm \cdots$$

が x の m 個の異なる値に対して成り立つことになる．こうして m 次の多項式

$$p(t) = \binom{2m+1}{1} t^m - \binom{2m+1}{3} t^{m-1} \pm \cdots + (-1)^m \binom{2m+1}{2m+1}$$

に対して，m 個の異なる根

$$a_r = \cot^2\left(\tfrac{r\pi}{2m+1}\right) \qquad (r = 1, 2, \ldots, m)$$

が得られたことになる．それゆえ，多項式は

$$p(t) \;=\; \binom{2m+1}{1} \left(t - \cot^2\left(\tfrac{\pi}{2m+1}\right)\right) \cdot \cdots \cdot \left(t - \cot^2\left(\tfrac{m\pi}{2m+1}\right)\right)$$

と一致する．そこで $p(t)$ における t^{m-1} の係数を比較すると，根の和は

$m = 1, 2, 3$ のときは
$\cot^2 \frac{\pi}{3} = \frac{1}{3}$
$\cot^2 \frac{\pi}{5} + \cot^2 \frac{2\pi}{5} = 2$
$\cot^2 \frac{\pi}{7} + \cot^2 \frac{2\pi}{7} + \cot^2 \frac{3\pi}{7} = 5$
となる．

係数比較：
$p(t) = c(t - a_1) \cdots (t - a_m)$ であれば，t^{m-1} の係数は $-c(a_1 + \cdots + a_m)$ である．

$$a_1 + \cdots + a_r = \frac{\binom{2m+1}{3}}{\binom{2m+1}{1}} = \frac{2m(2m-1)}{6}$$

となる．これで (1) が証明された．

もう1つ，コセカント関数 $\csc x = \frac{1}{\sin x}$ に対する，同じタイプの恒等式

$$\csc^2\left(\tfrac{\pi}{2m+1}\right) + \csc^2\left(\tfrac{2\pi}{2m+1}\right) + \cdots + \csc^2\left(\tfrac{m\pi}{2m+1}\right) = \frac{2m(2m+2)}{6} \qquad (3)$$

も必要となる．しかし，

$$\csc^2 x = \frac{1}{\sin^2 x} = \frac{\cos^2 x + \sin^2 x}{\sin^2 x} = \cot^2 x + 1$$

だから，(1) から (3) は，式の両辺に m を足すことで得ることができる．

さて，舞台は整い，準備完了である．$0 < y < \frac{\pi}{2}$ の範囲では

$0 < a < b < c$ から $0 < \frac{1}{c} < \frac{1}{b} < \frac{1}{a}$ が出る．

$$0 < \sin y < y < \tan y$$

であり，

$$0 < \cot y < \frac{1}{y} < \csc y$$

となって，

$$\cot^2 y < \frac{1}{y^2} < \csc^2 y$$

となる．この2重の不等式を，m 個の異なる x の値に適用して，足し合わせる．左辺については (1) を使い，右辺については (3) を使うと，

$$\frac{2m(2m-1)}{6} < \left(\tfrac{2m+1}{\pi}\right)^2 + \left(\tfrac{2m+1}{2\pi}\right)^2 + \cdots + \left(\tfrac{2m+1}{m\pi}\right)^2 < \frac{2m(2m+2)}{6}$$

となる．つまり，

$$\frac{\pi^2}{6}\frac{2m}{2m+1}\frac{2m-1}{2m+1} < \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{m^2} < \frac{\pi^2}{6}\frac{2m}{2m+1}\frac{2m+2}{2m+1}$$

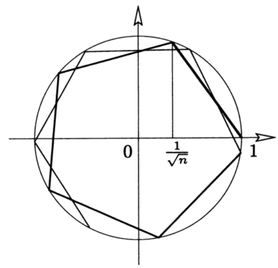
となる．左辺も右辺も，$m \longrightarrow \infty$ に従って $\frac{\pi^2}{6}$ に収束する．これで証明は終わり． □

さて次の定理が，無理数性について述べる最後の結果である．

定理 4. **あらゆる奇数 $n \geq 3$ に対して，数**

$$A(n) \quad = \quad \frac{1}{\pi}\arccos\left(\frac{1}{\sqrt{n}}\right)$$

は無理数である．



$n=3$ と $n=9$ の場合のヒルベルトの第 3 問題（第 7 章参照）に対してはこの結果が必要となる．$n=2$ と $n=4$ のときは，$A(2)=\frac{1}{4}$ と $A(4)=\frac{1}{3}$ となるので，奇数に制限するのは本質的である．これらの値は余白の図式に訴えれば容易に導くことができる．この図式では，「$\frac{1}{\pi}\arccos\left(\frac{1}{\sqrt{n}}\right)$ が無理数である」ことは，$\frac{1}{\sqrt{n}}$ から，各弦の長さが同じになるように多角形状に線で結んでいくときに，決して閉じることがない，ということと同値である．

$A(n)$ が有理数になるのは $n \in \{1,2,4\}$ に対してだけであるのを示すことは，読者の演習問題として残しておく．そのためには，$n=2^r$ の場合と n が 2 のベキでない場合とを区別すること．

■ **証明.** 初等的な三角法から加法定理

$$\cos\alpha + \cos\beta = 2\cos\tfrac{\alpha+\beta}{2}\cos\tfrac{\alpha-\beta}{2}$$

を使う．$\alpha=(k+1)\varphi, \beta=(k-1)\varphi$ とおくと，

$$\cos(k+1)\varphi \quad = \quad 2\cos\varphi\,\cos k\varphi \;-\; \cos(k-1)\varphi \qquad (4)$$

となる．これから，$\cos\varphi_n = \frac{1}{\sqrt{n}}$ $(0 \leq \varphi_n \leq \pi)$ によって定義される角 $\varphi_n = \arccos\left(\frac{1}{\sqrt{n}}\right)$ に対して，

$$\cos k\varphi_n \quad = \quad \frac{A_k}{\sqrt{n}^k}$$

という形の表示が得られる．ここで，すべての $k \geq 0$ に対して，A_k は n で割れない整数である．実際，$k=0,1$ に対しては $A_0=A_1=1$ であり，そういう表示がある．k に関する帰納法により，(4) を使うと，$k \geq 1$ に対して

$$\cos(k+1)\varphi_n \quad = \quad 2\frac{1}{\sqrt{n}}\frac{A_k}{\sqrt{n}^k} - \frac{A_{k-1}}{\sqrt{n}^{k-1}} \quad = \quad \frac{2A_k - nA_{k-1}}{\sqrt{n}^{k+1}}$$

となる．こうして，$A_{k+1} = 2A_k - nA_{k-1}$ が得られる．もし $n \geq 3$ が

奇数で，A_k が n で割れないならば，A_{k+1} もまた n で割ることができない．

ここで，

$$A(n) = \frac{1}{\pi}\varphi_n = \frac{k}{\ell}$$

が有理数であると仮定する（整数 $k, \ell > 0$）．すると，$\ell\varphi_n = k\pi$ であり，

$$\pm 1 = \cos k\pi = \cos \ell\varphi_n = \frac{A_\ell}{\sqrt{n}^\ell}$$

が得られる．こうして，$\ell \geq 2$ に対して $\sqrt{n}^\ell = \pm A_\ell$ は整数になり，それゆえ $n \,|\, \sqrt{n}^\ell$ となる．$\sqrt{n}^\ell \,|\, A_\ell$ だから n が A_ℓ を割ることになり，これは矛盾である．□

附録：リーマンのゼータ関数

リーマンのゼータ関数 $\zeta(s)$ は実数 $s > 1$ に対しては

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

によって定義される．H_n に対する評価（14 ページ参照）から，$\zeta(1)$ に対する級数は発散するが，任意の実数 $s > 1$ に対しては収束することがわかる．ゼータ関数は全複素平面に（$s = 1$ に 1 位の極を 1 つ持つが）標準的に解析接続される．これはベキ級数展開によって構成することができる．得られる複素関数は，素数の理論に対してこの上ない重要性を持っている．関連する話題を 3 つ述べておこう．

(1) 注目すべきオイラーの恒等式

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

は，あらゆる自然数が一意的な (!) 素因数分解を持つことを凝縮したものになっている．つまり，この基本的な事実を使うと，公式は等比級数展開

$$\frac{1}{1 - p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots$$

から，簡単に導かれる．

(2) ゼータ関数の複素零点の配置は，全数学において，もっとも有名で重要な未解決予想の 1 つである「リーマン予想」のテーマである．それは，ゼータ関数の自明でない零点 $s \in \mathbb{C}$ はすべて

$$\mathrm{Re}(s) \;=\; \frac{1}{2}$$

を満たすというものである.（ゼータ関数はすべての負の偶数で 0 になり，それらを「自明な零点」と呼ぶことにする.）

ごく最近，ジェフ・ラガリアスは驚くべきことを発見した．リーマン予想は次の初等的な主張と同値だというのである.「すべての $n \geq 1$ に対して，

$$\sum_{d \mid n} d \;\leq\; H_n \;+\; \exp(H_n)\log(H_n)$$

が成り立つ．ここで，H_n は前のように n 番目の調和数であり，等式が成り立つのは $n = 1$ のときだけである.」

(3) 長い間，s が**偶数**で，$s \geq 2$ であれば，$\zeta(s)$ は π^s の有理数倍で，それゆえ無理数であることが知られていた（第 19 章参照）．この章では，1734 年の有名なオイラーの恒等式 $\zeta(2) = \frac{\pi^2}{6}$ の 2 つの天書の証明を提示した．対照的に，$\zeta(3)$ の無理数性は，1979 年にロジェ・アペリーによって証明されたばかりである（[10] の素晴らしい概説記事を参照のこと）．少なからぬ努力にもかかわらず，他の奇数 $s = 2t + 1 \geq 5$ に対しては，$\zeta(s)$ についての状況は完全とはほど遠いものだった．これに関する最新の数学的ニュースはリヴォーの論文で，値 $\zeta(2t + 1)$ のうち無限個が無理数であるというものである．

参考文献

[1] T. M. アポストル：「オイラーの失われた証明：やさしく $\zeta(2)$ の値を求めること」(*A proof that Euler missed: Evaluating* $\zeta(2)$ *the easy way*), Math. Intelligencer **5** (1983), 59-60.

[2] K. ボール，T. リヴォー：「奇数におけるゼータ関数の無限個の値の無理数性」(*Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs*), Inventiones math. **146** (2001), 193-207.

[3] F. ボイカーズ，A. C. コルク，E. カラビ：「一般の調和級数の和と体積」(*Sums of generalized harmonic series and volumes*), Nieuw Archief voor Wiskunde (4) **11** (1993), 217-224.

[4] C. エルミート：「指数関数について」(*Sur la fonction exponentielle*), Comptes rendus de l'Académie des Sciences (Paris) **77** (1873), 18-24; Œuvres de Charles Hermite, Vol. III, Gauthier-Villars, Paris 1912, pp. 150-181.

[5] 岩本義和：「π^2 が無理数であることの証明」(*A proof that π^2 is irrational*), J. Osaka Institute of Science and Technology **1** (1949), 147-148.

[6] J. F. コクスマ：「π が無理数であることのニーヴンの証明」(*On Niven's proof that π is irrational*), Nieuw Archiv Wiskunde (2) **23** (1949), 39.

[7] J. C. ラガリアス：「リーマン仮説と同値な初等的問題」(*An elementary problem equivalent to the Riemann hypothesis*), Amer. Math. Monthly **109** (2002), 534-543.

[8] W. J. ルヴェク：『数論の話題　第I巻』(*Topics in Number Theory, Vol. I*), Addison-Wesley, Cambridge MA 1956.

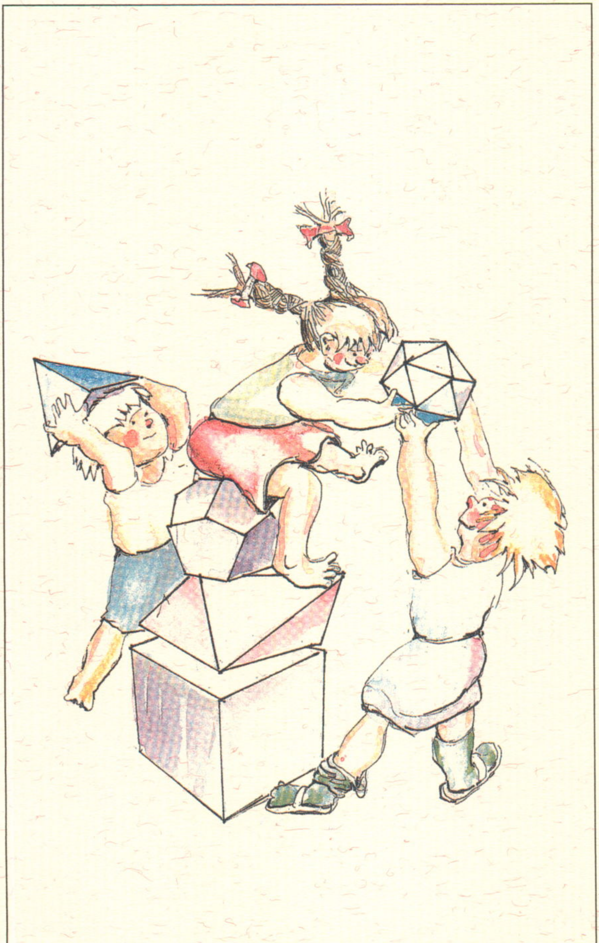
[9] I. ニーヴン：「π が無理数であることの簡単な証明」(*A simple proof that π is irrational*), Bulletin Amer. Math. Soc. **53** (1947), 509.

[10] A. ファン・デル・ポルテン：「オイラーが失った証明 ... $\zeta(3)$ の無理数性のアペリーの証明．非公式な報告」(*A proof that Euler missed ... Apéry's proof of the irrationality of $\zeta(3)$. An informal report*), Math. Intelligencer **1** (1979), 195-203.

[11] T. J. ランズフォード：「$\sum_1^\infty \frac{1}{n^2} = \frac{\pi^2}{6}$ の初等的証明」(*An elementary proof of $\sum_1^\infty \frac{1}{n^2} = \frac{\pi^2}{6}$*), Eureka No. 42, Summer 1982, 3-5.

[12] A. M. ヤグロム，I. M. ヤグロム:『初等的な解がある挑戦的な数学の問題　第2巻』(*Challenging mathematical problems with elementary solutions, Vol. 2*), Holden-Day, San Francisco 1967.

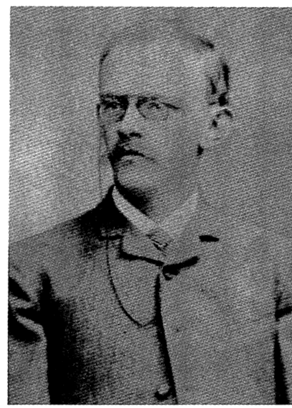
幾何学



「プラトンの立体 —— 子供の遊び!」

第7章　ヒルベルトの第3問題：多面体を分割する

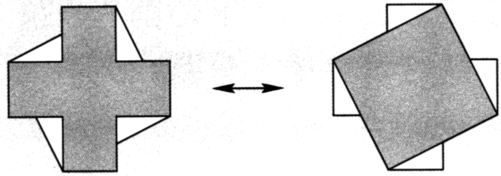
1900年のパリの国際数学者会議における伝説となった講演の中で，ダーフィト・ヒルベルトは，23の問題の中の3番目として，


ダーフィト・ヒルベルト

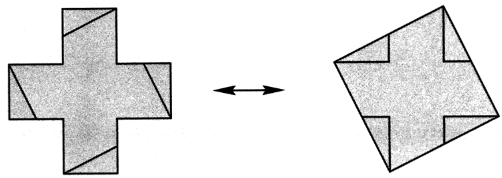
> 「等しい底面積と等しい高さを持つ2つの4面体で，どのようにしても合同な4面体たちに分割することもできず，また合同な4面体を付け加えてできるどんな2つの多面体も，それら自身合同な4面体たちに分割できないもの」

があるかどうかを問題とした．

この問題は，1844年のカール・フリードリッヒ・ガウスの2通の手紙（1900年のガウスの全集所収）に遡ることができる．もし等しい体積の4面体を合同な部分に分割することができるのなら，底面積と高さが同じピラミッドは同じ体積を持つという，ユークリッドの定理XII.5の「初等的」な証明が得られるだろう．そうであれば，多面体の体積に対する初等的な定義（解析学によらず，それゆえ連続性の議論を使わないもの）が得られることになる．平面幾何でなら同様の主張は正しい．つまり，ボヤイ–ゲルウィーンの定理[1, 第2.7節]によれば，平面の多角形が**分割合同**である（合同な三角形たちに分割できる）ことと，**補充合同**である（合同な三角形たちを付け加えて合同にすることができる）ことの双方は，同じ面積を持つことと同値である．



十字形は同じ面積の正方形と補充合同である.



実際，分割合同でもある.

問題の言い回しからわかるように，ヒルベルトは，3次元では類似の定理が成り立たないと思っていたようで，それは正しかったのだ．実際，問題はヒルベルトの弟子のマクス・デーンの2つの論文によって完全に解決された．等しい底面積と高さを持つ分割合同でない4面体を示した最初のものは，すでに1900年に出ており，さらに補充合同についても扱っている第2の論文は1902年に出ている．しかし，デーンの論文は理解しやすいものでなく，他の人たちがかかった微妙な罠に落ち込んでいないかどうかを見るには努力が必要だった．非常にエレガントだが不幸にも間違っている証明が，ブリカード（1896年！）やメシュコフスキー(1960)によって，おそらくはその他の人によっても与えられてきた．幸運なことに，デーンの証明は研究し直され，V. F. カガン(1903/1930)，ヒューゴー・ハドヴィガー(1949/54)，ヴラディーミル・G・ボルチャンスキーの努力を合わせることによって，以下のような天書の証明が得られている．（本章の附録に，多面体に関する基本的なことがらを与えておく.）

(1) 線形代数を少々

実数の任意の有限集合 $M = \{m_1, \dots, m_k\} \subseteq \mathbb{R}$ に対して，M に属する数の有理係数の線形結合全体の集合として $V(M)$ を定義する．つまり，

$$V(M) = \left\{ \sum_{i=1}^{k} q_i m_i : q_i \in \mathbb{Q} \right\} \subseteq \mathbb{R}$$

とおく．

（自明だが，重要なこととして）まずわかることは，$V(M)$ が有理数体 $\mathbb{Q}$ 上の有限次元ベクトル空間であるということである．実際，$V(M)$ は明らかに和をとることと，有理数を掛けることに関して閉じており，$\mathbb{R}$ に対する体の公理によって $V(M)$ はベクトル空間になる．$V(M)$ の次元は，極小な生成集合の大きさになる．定義により，M は $V(M)$ を生成するので，ある極小な生成集合を含むことになる．それゆえ，

$$\dim_{\mathbb{Q}} V(M) \leq k = |M|$$

となる．以下で，$\mathbb{Q}$ ベクトル空間の線形写像と解釈することのできる，**$\mathbb{Q}$ 線形関数**

$$f : V(M) \to \mathbb{Q}$$

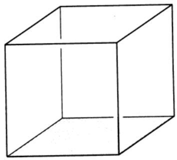
を使う必要がでてくる．鍵になる性質は，有理線形従属性 $\sum_{i=1}^{k} q_i m_i = 0$ ($q_i \in \mathbb{Q}$) があると，$\sum_{i=1}^{k} q_i f(m_i) = f(0) = 0$ が成り立たねばならないということである．次の単純な補題も成り立つが，これはあとで使うことになる．

補題．$\mathbb{R}$ の任意の有限部分集合 $M \subseteq M'$ に対して，$\mathbb{Q}$ ベクトル空間 $V(M)$ は $\mathbb{Q}$ ベクトル空間 $V(M')$ の部分空間である．$f : V(M) \to \mathbb{Q}$ が $\mathbb{Q}$ 線形関数であれば，f は $\mathbb{Q}$ 線形関数 $f' : V(M') \to \mathbb{Q}$ に，$f'(m) = f(m)$ $(m \in M)$ を満たすように拡張することができる．

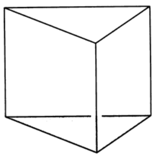
■ **証明．** どんな $\mathbb{Q}$ 線形関数 $V(M) \to \mathbb{Q}$ も，$V(M)$ の $\mathbb{Q}$ 基底での値を定めれば決まるが，$V(M)$ のあらゆる基底は $V(M')$ の基底に拡張できる． □

(2) デーン不変量

3 次元多面体 P に対して，隣り合う面の間の角（**2 面角**）と数 π を合わせた集合を M_P と表わす．立方体 C に対しては，$M_C = \left\{\frac{\pi}{2}, \pi\right\}$ であり，正三角形を底面とする直交プリズム Q に対しては，$M_Q = \left\{\frac{\pi}{3}, \frac{\pi}{2}, \pi\right\}$ となる．



$M_C = \{\frac{\pi}{2}, \pi\}$



$M_Q = \{\frac{\pi}{3}, \frac{\pi}{2}, \pi\}$

M_P を含む任意の有限集合 $M \subseteq \mathbb{R}$ と，$f(\pi) = 0$ を満たす任意の $\mathbb{Q}$ 線形関数

$$f : V(M) \to \mathbb{Q}$$

が与えられるとき，P の（f に関する）**デーン不変量**を実数

$$D_f(P) \;=\; \sum_{e \in P} \ell(e) \cdot f(\alpha(e))$$

として定義する．ここで，和は多面体のすべての稜 e に関してとり，$\ell(e)$ を e の長さとし，$\alpha(e)$ を e で交わる 2 つの面の間の角とする．

あとで色々なデーン不変量を計算する．今のところは，**任意の**このような $\mathbb{Q}$ 線形関数 f に対して $f\left(\frac{\pi}{2}\right) = \frac{1}{2}f(\pi) = 0$ とならねばならないので，

$$D_f(C) \;=\; 0$$

つまり，立方体のデーン不変量は**任意の** f に関して 0 になることを注意しておくだけにする．

(3) デーン–ハドヴィガーの定理

上でしたように，2 つの多面体 P, Q が**分割合同**であると言うのを，それらが有限個の多面体の集合 $P_1, \ldots, P_n$ と $Q_1, \ldots, Q_n$ に分割され，すべての i $(1 \leq i \leq n)$ に対して P_i と Q_i が合同であるときとする．2 つの多面体が**補充合同**であると言うのを，多面体 $P_1, \ldots, P_m$ と $Q_1, \ldots, Q_m$ が存在して，P_i の内部が他のものや P とも交わりを持たず，Q_i と Q に対しても同様で，すべての i に対して P_i と Q_i が合同であり，$\widetilde{P} = P \cup P_1 \cup P_2 \cup \cdots \cup P_m$ と $\widetilde{Q} = Q \cup Q_1 \cup Q_2 \cup \cdots \cup Q_m$ が分割合同であるときとする．1844 年のゲルリンクの定理によれば，合同を考える際に鏡映を許すかどうかには関係がない．

明らかに，分割合同な多面体は補充合同であるが，逆は明らかとは言い難い．次のハドヴィガーの定理（ボルチャンスキー版のもの）は，ヒルベルトが提案したように，補充合同でなくしたがって分割合同でない，体積の等しい 4 面体を見つけるための道具を与えてくれる．

定理． **P と Q を多面体で，その稜での 2 面角をそれぞれ $\alpha_1, \ldots, \alpha_p$ と $\beta_1, \ldots, \beta_q$ とし，M を**

$$\{\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q, \pi\} \subseteq M$$

を満たす実数の有限集合とする．もし $\mathbb{Q}$ 線形関数 $f : V(M) \to \mathbb{Q}$ で $f(\pi) = 0$ と

$$D_f(P) \neq D_f(Q)$$

を満たすものがあれば，P と Q は補充合同ではない．

■ **証明.** 議論は 2 つの部分に分かれる．

(1) もし多面体 P が有限個の多面体の部分 $P_1, \ldots, P_n$ に分割され，各部分 $P_1, \ldots, P_n$ の 2 面角が集合 M に含まれていれば，あらゆる $\mathbb{Q}$ 線形関数 $f : V(M) \to \mathbb{Q}$ に対して，デーン不変量を足し合わせると，

$$D_f(P) \;=\; D_f(P_1) + \cdots + D_f(P_n)$$

となる．

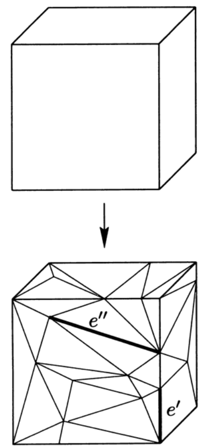
これを示すために，多面体の稜の任意の部分に**質量**を付与する．つまり，$e' \subseteq e$ が多面体 P の稜 e の部分であれば，その質量は，その 2 面角の f 値に長さを掛けたもの

$$m_f(e') \;=\; \ell(e')\, f(\alpha(e'))$$

とする．

さて，P が $P_1, \ldots, P_n$ と分割されているなら，部分 P_i の稜のすべての和集合を考える．P の稜に含まれている稜 e' に沿って，部分の 2 面角を足し合わせると e' での P の 2 面角になり，それゆえ質量も同じように足し合わされることがわかる．

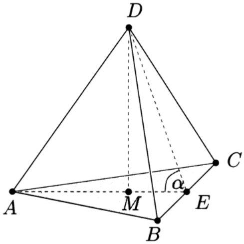
それ以外の，P のある面の内部か P の内部に含まれるような，ある P_i の稜 e'' のところで角を足せば，π か 2π かになる．だから，部分における角の f 値を足し合わせれば，それぞれ $f(\pi) = 0$ か $f(2\pi) = 0$ になる．こうして質量の和については，これらの稜に対し，P に対して最初の場所で与えた質量と同じ値，つまり 0 になる．



(2) P と Q が補充合同であると仮定すると，問題になるどれかの部分に現れる 2 面角をすべて含むような，M を含む集合 M' を考えることができる．有限の分割しか考えていないから，M' は有限集合である．そのとき補題によって，f を $f' : V(M') \to \mathbb{Q}$ に拡張することができ，(1) によって

$$D_{f'}(P)+D_{f'}(P_1)+\cdots+D_{f'}(P_m)=D_{f'}(Q)+D_{f'}(Q_1)+\cdots+D_{f'}(Q_m)$$

の型の等式が得られる．ここで，P_i と Q_i は合同だから，$D_{f'}(P_i)=D_{f'}(Q_i)$ である．それゆえ，$D_f(P)=D_f(Q)$ となるが，これは矛盾である． □



例 1. 稜の長さが ℓ の正4面体 T_0 に対して，スケッチから2面角を計算しよう．底面の中点 M は底面の三角形の高さ AE を $1:2$ に内分し，$|AE|=|DE|$ だから，$\cos\alpha=\frac{1}{3}$ となり，つまり，

$$\alpha = \arccos\frac{1}{3}$$

となる．$M=\{\alpha,\pi\}$ とおくと，比

$$\frac{\alpha}{\pi} = \frac{1}{\pi}\arccos\frac{1}{3}$$

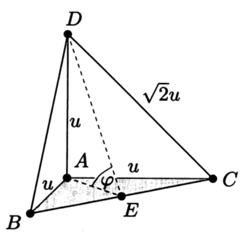
は，第6章定理4によって（$n=9$ とおいて），無理数となることを注意しておく．こうして，$\mathbb{Q}$ ベクトル空間 $V(M)$ は2次元で，基底 M を持ち，$\mathbb{Q}$ 線形関数 $f:V(M)\to\mathbb{Q}$ で

$$f(\alpha)=1,\quad f(\pi)=0$$

を満たすものが存在する．この f に対して，

$$D_f(T_0) = 6\ell f(\alpha) = 6\ell \neq 0$$

となり，立方体のデーン不変量がどんな f に対しても0だったから，**正4面体は立方体と，分割合同にも補充合同にもなり得ない．**



例 2. T_1 を，長さ u の直交する3つの稜 AB, AC, AD で張られる4面体とする．この4面体の2面角は，直角が3つと，スケッチから以下のように計算される同じ大きさ φ が3つである．まず，

$$\cos\varphi = \frac{|AE|}{|DE|} = \frac{\frac{1}{2}\sqrt{2}u}{\frac{1}{2}\sqrt{3}\ \sqrt{2}u} = \frac{1}{\sqrt{3}}$$

であり，これから

$$\varphi = \arccos\frac{1}{\sqrt{3}}$$

となる．

$M = \left\{\frac{\pi}{2}, \arccos\frac{1}{\sqrt{3}}, \pi\right\}$ に対して，$\mathbb{Q}$ ベクトル空間 $V(M)$ は 2 次元である．実際，π と $\frac{\pi}{2}$ は 1 次従属だから $V(M) = V\left(\left\{\arccos\frac{1}{\sqrt{3}}, \pi\right\}\right)$ となるが，第 6 章で証明したように（定理 4 で $n = 3$ とおく），$\arccos\frac{1}{\sqrt{3}}$ と π の間にはどんな有理関係もなく，同じことだが，$\frac{1}{\pi}\arccos\frac{1}{\sqrt{3}}$ は無理数である．

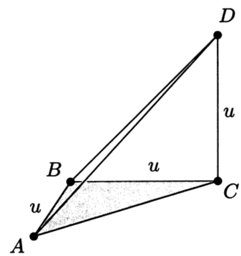
こうして，$\mathbb{Q}$ 線形写像 f を

$$f(\pi) = 0 \quad \text{かつ} \quad f\left(\arccos\frac{1}{\sqrt{3}}\right) = 1$$

とおいて与えると，$f(\frac{\pi}{2}) = 0$ が得られ，それゆえ，

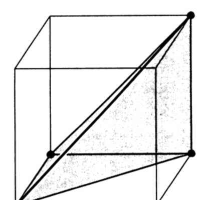
$$D_f(T_1) \;=\; 3uf\left(\tfrac{\pi}{2}\right) + 3(\sqrt{2}u)f\left(\arccos\tfrac{1}{\sqrt{3}}\right) \;=\; 3\sqrt{2}u \;\neq\; 0$$

となる．このことによって，T_1 は同じ体積の立方体 C と分割合同でも補充合同でもない．というのも，**任意の** f に対しては $D_f(C) = 0$ となるからである．



例 3. 最後に，4 面体 T_2 を，同じ長さ u の互いに直交する連続した稜 AB, BC, CD を持つもの（「直交スキーム」）とする．

このような 4 面体の角は計算しないで（角は $\frac{\pi}{2}$, $\frac{\pi}{3}$, $\frac{\pi}{4}$ である），むしろ稜と面の中点と中心を使って，稜の長さが u の立方体がこの型の 6 つの 4 面体（合同なものが 3 つと鏡像が 3 つ）に分割することができるという議論をする．



これらすべての合同なものと鏡像は同じデーン不変量を持つので，あらゆる適当な関数 f に対して

$$D_f(T_2) = \frac{1}{6}D_f(C) = 0$$

となり，それゆえこのような 4 面体のすべてのデーン不変量は 0 になる！これでヒルベルトの第 3 問題が解かれたことになる．なぜなら，前に別の 4 面体 T_1 で，底面が合同，高さが同じで，$D_f(T_1) \neq 0$ であるものを構成した．デーン–ハドヴィガーの定理によって，T_1 と T_2 は分割合同でなく，補充合同ですらない．

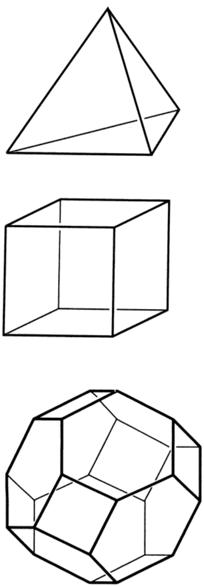
附録：多面体

$\mathbb{R}^d$ の**凸多面体**とは有限集合 $S = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n\}$ の凸包，つまり

$$P \;=\; \mathrm{conv}(S) \;=\; \Big\{ \sum_{i=1}^{n} \lambda_i \boldsymbol{s}_i : \lambda_i \geq 0,\ \sum_{i=1}^{n} \lambda_i = 1 \Big\}$$

の形の集合のことである．多面体は確かになじみの深い対象である．主な例は，**凸多角形**（2 次元の凸多面体）や（3 次元の）**凸多面体**である．

多面体を自然に高次元に拡張するにはいくつかのタイプがある．たとえば，S が濃度 $d+1$ のアフィン独立な集合であれば，$\mathrm{conv}(S)$ は d 次元**単体**（または d **単体**）である．$d=2$ のときは三角形で，$d=3$ のときは 4 面体である．同じように，正方形や立方体は，$C_d = [0,1]^d \subseteq \mathbb{R}^d$ で与えられる**単位 d 立方体**のような d 立方体の特殊な場合になっている．



なじみの多面体をいくつか：4 面体，立方体，交換多面体．

一般の多面体は凸多面体の有限和として定義される．本書では，凸でない多面体は第 11 章のコーシーの剛性定理との関係で出てくるし，凸でない多角形は第 10 章のピックの定理との関係で出てくる．また，第 28 章の美術館（ギャラリー）の定理を述べる際にも出てくる．

凸多面体はまた，同値だが，線形不等式の有限系の有界な解集合として定義することもできる．こうして，あらゆる凸多面体 $P \subseteq \mathbb{R}^d$ には，ある行列 $A \in \mathbb{R}^{m \times d}$ とベクトル $\boldsymbol{b} \in \mathbb{R}^m$ に対して

$$P \;=\; \{\boldsymbol{x} \in \mathbb{R}^d : A\boldsymbol{x} \leq \boldsymbol{b}\}$$

という形の表示がある．言い換えれば，$\boldsymbol{a}_i^T$ を A の第 i 行とするとき，m 個の線形不等式の系 $\boldsymbol{a}_i^T \boldsymbol{x} \leq b_i$ の解集合である．逆に，そのようなあらゆる有限の解集合は凸多面体であり，有限の点集合の凸包として表わすことができる．

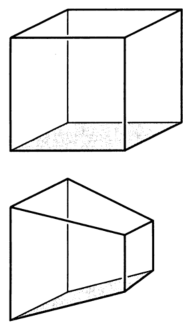
2 次元と 3 次元の多面体に対しては，**頂点**，**辺または稜**，**2 次元面**という概念に親しんでいる．高次元の凸多面体に対しては，以下のように面を定義することができる．P の**面**とは，$P \cap \{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{a}^T \boldsymbol{x} = b\}$ という形の部分集合 $F \subseteq P$ のことである．ここで，$\boldsymbol{a}^T \boldsymbol{x} \leq b$ はすべての点 $\boldsymbol{x} \in P$ に対して成り立つ線形不等式である．

多面体のすべての面はまた多面体である．凸多面体の頂点（0 次元面）

の集合 V は $\mathrm{conv}(V) = P$ を満たす，包含関係に関して極小な集合でもある．$P \subseteq \mathbb{R}^d$ を d 次元の凸多面体であると仮定すると，$(d-1)$ 次元面は，超平面の極小な集合で，だから P を含む半空間の集合で，共通部分が P になるような極小の集合を定める．このことから特に，あとで必要となる次の事実が成り立つ.「F を P の $(d-1)$ 次元面とし，それの定める超平面を H_F と書き，H_F を境界とする 2 つの閉じた半空間を H_F^+ と H_F^- と書く．すると，この 2 つの半空間のうち，1 つが P を含む（が，もう 1 つは含まない）.」

凸多面体 P のグラフ $G(P)$ は，頂点の集合 V と辺（稜）の集合 E で与えられるものである．P が 3 次元なら，このグラフは平面グラフで，そのことから有名な「オイラーの多面体公式」（第 10 章参照）が得られる．

2 つの多面体 $P, P' \subseteq \mathbb{R}^d$ が**合同**であるのは，P を P' に写す長さを保つアフィン写像が存在するときである．そのような写像は空間の向き付けを変えるかも知れない．たとえば，ある超平面に関する P の鏡映は，P を P の**鏡像**に写す．それらが**組合せ同値**であるのは，P の面の集合から P' の面の集合への全単射で，次元を保ち，面の間の包含関係を保つものが存在するときである．この組合せ同値の概念は合同よりずっと弱い概念である．たとえば，余白の図は単位立方体と，それに組合せ同値な「歪」立方体（それで，このようなものも「立方体」と呼ぶ）を示したものだが，これらはもちろん合同でない．



組合せ同値な多面体.

多面体（または $\mathbb{R}^d$ のより一般な部分集合）が**中心対称**であるのは，ある点 $\boldsymbol{x}_0 \in \mathbb{R}^d$ があって，

$$\boldsymbol{x}_0 + \boldsymbol{x} \in P \quad \Longleftrightarrow \quad \boldsymbol{x}_0 - \boldsymbol{x} \in P$$

を満たすときである．このとき，$\boldsymbol{x}_0$ を P の**中心**と言う．

参考文献

[1] V. G. ボルチャンスキー：『ヒルベルトの第 3 問題』(*Hilbert's Third Problem*), V. H. Winston & Sons (Halsted Press, John Wiley & Sons), Washington DC 1978.

[2] M. デーン：「空間的に同じ多面体について」(*Ueber raumgleiche Polyeder*), Nachrichten von der Königl. Gesellschaft der Wissenschaften, Mathematisch-physikalische Klasse (1900), 345-354.

[3] M. デーン：「体積について」(*Ueber den Rauminhalt*), Mathematische Annalen **55** (1902), 465-478.

[4] C. F. ガウス：「合同と対称性：ゲルリンクとの往復書簡」(*"Congruenz und Symmetrie": Briefwechsel mit Gerling*), 『全集第8巻』(Werke, Band VIII), Königl. Gesellschaft der Wissenschaften zu Göttingen; B. G. Teubner, Leipzig (1900), 240-249.

[5] D. ヒルベルト：「数学の問題」(*Mathematical Problems*), 1900年のパリの国際数学者会議における講演, Bulletin Amer. Math. Soc. **8** (1902), 437-479.

[6] G. M. ツィーグラー：『多面体講義』(*Lectures on Polytopes*), Graduate Texts in Mathematics **152**, Springer-Verlag New York 1995.

第8章　平面の中の直線とグラフの分割

直線の配置に関して最もよく知られている問題はおそらく，1893 年に数学の問題のコラムでシルヴェスターによって述べられた次のものであろう．



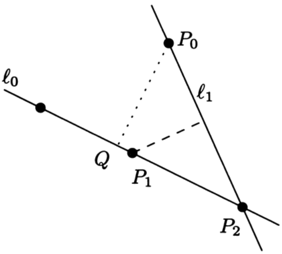
J. J. シルヴェスター

> **解くべき問題**
>
> **11851.**（シルヴェスター教授）任意有限個の実の点をうまく配置して，その内の 2 点を通る直線がいつも第 3 の点を通るようにすることは，すべての点が同じ 1 つの直線の中にあるとき以外は不可能であることを証明せよ．

シルヴェスター自身が証明を持っていたかは疑問だが，正しい証明が 40 年ほどのちにティボー・ガライ［グリュンヴァルド］によって与えられた．そのため，以下の定理はシルヴェスター–ガライの定理とされることが多い．ガライの証明のあと，いくつか証明も発表されたが，L. M. ケリーによる以下の議論がおそらく「単純で最良」なものだろう．

定理 1. 平面において，1 直線上にない n 個の点をどのように配置しても，そのうちちょうど 2 個の点しか含まないような直線が存在する．

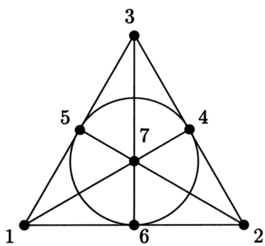
■ **証明.** $\mathcal{P}$ を与えられた点の集合とし，$\mathcal{P}$ の少なくとも 2 点を通る直線全体の集合 $\mathcal{L}$ を考えよう．点 P が直線 ℓ に属さないようなすべての対 (P,ℓ) の中から，P_0 から ℓ_0 までの距離が最小であるような対 (P_0,ℓ_0)



を選んで，Q を P_0 に最も近い ℓ_0 上の点とする（つまり，Q と P_0 を通る直線は ℓ_0 に垂直である）．

主張．この直線 ℓ_0 が実現している！

もしそうでなければ，ℓ_0 は $\mathcal{P}$ の点を少なくとも3つ含んでおり，そのうちの2つは Q を境とした同じ側にあることになる．それを P_1 と P_2 とする．P_1 が Q と P_2 の間にあると仮定しよう．P_1 と Q が同じ点であることもあり得る．この配置は余白の図のようになっている．このことから，P_0 と P_2 によって定まる直線 ℓ_1 と P_1 との距離は，P_0 と ℓ_0 との距離より小さくなる．これは ℓ_0 と P_0 の取り方に矛盾する．　□



証明では，実平面の計量公理（最短距離）と順序公理（P_1 は Q と P_2 の間にある）を使った．点と直線の通常の結合公理以上に，これらの性質が本当に必要なのだろうか？ 余白に描かれた有名なファノ平面[1]が示しているように，何かしらの余分な条件が必要となる．そこでは，$\mathcal{P}=\{1,2,\ldots,7\}$ であり，$\mathcal{L}$ は図に示したように7つの3点直線からなっている．その中には $\{4,5,6\}$ という「直線」も入っている．どの2点も直線を一意的に定め，結合公理は満たされているが，2点直線は存在しない．したがって，シルヴェスター–ガライの定理は，ファノの配置を実平面の中に埋め込んで，7つの共線的な3つ組が実直線上に乗っているようにすることができないことを示している．どうしても「曲がった」直線が出てくることになる．

しかしながら，シルヴェスター–ガライの定理の証明には順序公理があれば十分であることが，コクセターによって証明されている．つまり，どんな計量公理も使わないような証明を工夫することができるのである．第10章で与える，オイラーの公式を使った証明も参照のこと．

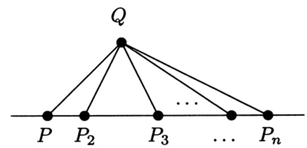
シルヴェスター–ガライの定理からすぐに，平面の点と直線に関するもう1つの有名な結果が導かれる．それはポール・エルデシュとニコラス・G・ド・ブリュインによるものである．しかしこの場合，彼らがすでに注意しているように，結果はもっと一般に任意の点・線系に対して成り立っている．そのあとすぐに，より一般な結果を述べることにしよう．

---

[1] ［訳註］有限標数の体の上でも射影幾何が考えられるが，標数2の射影平面にはファノの公理が成り立つ．それを平面上に実現したモデルが余白の図である．点は7つ，直線も7つである．点4,5,6を通っている円はその幾何では直線である．詳しくはたとえば，シャファレヴィッチ著『代数学とは何か』（シュプリンガー・フェアラーク東京，2001）の第10章参照．

定理 2. **$\mathcal{P}$ を平面の $n \geq 3$ 個の点の集合で，すべてが 1 つの直線上にあるものではないとする．そのとき，少なくとも 2 つの $\mathcal{P}$ の点を通る直線の集合 $\mathcal{L}$ には，少なくとも n 本の直線がある．**

■ **証明.** $n = 3$ のときには示すべきことはない．n に関する帰納法で証明しよう．$|\mathcal{P}| = n + 1$ とする．前の定理によって，$\mathcal{P}$ のちょうど 2 つの点 P と Q を含んでいる直線 $\ell_0 \in \mathcal{L}$ が存在する．集合 $\mathcal{P}' = \mathcal{P} \backslash Q$ と $\mathcal{P}'$ によって定まる直線の集合 $\mathcal{L}'$ を考える．$\mathcal{P}'$ の点がすべて 1 つの直線上にあるのでないなら，帰納法によって $|\mathcal{L}'| \geq n$ であり，それゆえ，$\mathcal{L}$ にはもう 1 つの直線 ℓ_0 があるので，$|\mathcal{L}| \geq n + 1$ となる．一方，$\mathcal{P}'$ の点がすべて 1 つの直線の上にあるなら，「束（ペンシル）」ができて，ちょうど $n + 1$ 本の直線が得られる[2]． □



さて，約束した通り，ずっと一般な「結合の幾何」に適用することのできる一般的な結果を述べよう．

定理 3. **X を $n \geq 3$ 個の元からなる集合，$A_1, \ldots, A_m$ を X の真部分集合で，X の元の任意の対がある 1 つの集合 A_i だけに含まれているとする．そのとき，$m \geq n$ が成り立つ．**

■ **証明.** 以下の証明はいろんな形でモツキンとコンウェイに帰されるのだが，ほとんど 1 つの文だけからなり，実に見事なものである．$x \in X$ に対して，x を含む集合 A_i の数を r_x とする．(仮定により $2 \leq r_x < m$ となることに注意.) さて，$x \notin A_i$ なら $r_x \geq |A_i|$ である．なぜなら，A_i のある元と x とを含む $|A_i|$ 個の集合は異なっていなければならないからである．$m < n$ と仮定すると，$m|A_i| < n r_x$ となり，したがって，$x \notin A_i$ に対して $m(n - |A_i|) > n(m - r_x)$ となって，

$$1 = \sum_{x \in X} \frac{1}{n} = \sum_{x \in X} \sum_{A_i : x \notin A_i} \frac{1}{n(m - r_x)} > \sum_{A_i} \sum_{x : x \notin A_i} \frac{1}{m(n - |A_i|)} = \sum_{A_i} \frac{1}{m} = 1$$

となってしまう[3]．しかし，このようなことは起こらない． □

この定理にもう 1 つ，線形代数を使った非常に短い証明がある．B を

---

[2] ［訳註］ある直線の集合が 1 点 Q を通るとき，直線束ということがある．有限射影幾何でなら，1 点を通る直線の全体に対して用いられる．

[3] ［訳註］$|\{A_i \mid x \notin A_i\}| = m - r_x$ であり，$|\{x \in X \mid x \notin A_i\}| = n - |A_i|$ である．

$(X; A_1, \ldots, A_m)$ の**接続行列**とする．つまり，B の行は X の元で番号をつけ，列は $A_1, \ldots, A_m$ で番号をつけたもので，成分が

$$B_{xA} = \begin{cases} 1 & x \in A \text{ のとき} \\ 0 & x \notin A \text{ のとき} \end{cases}$$

であるものとする．積 BB^T を考える．$x \neq x'$ のときは，x と x' を含む集合 A_i はただ 1 つだから，$(BB^T)_{xx'} = 1$ となり，それゆえ

$$BB^T = \begin{pmatrix} r_{x_1}-1 & 0 & \cdots & 0 \\ 0 & r_{x_2}-1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & r_{x_n}-1 \end{pmatrix} + \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & 1 \end{pmatrix}$$

となる．ここで，r_x は上で定義したものである．最初の行列は正定値であり（固有値がすべて正），第 2 の行列は半正定値（固有値は n と 0）であるから，BB^T が正定値で，特に可逆で，$\mathrm{rank}(BB^T) = n$ であることが導かれる．このことから，$(n \times m)$ 行列 B は少なくともランク n であり，実際に $n \leq m$ となるという結論が得られる．ランクは列の数を超えることができないからである．

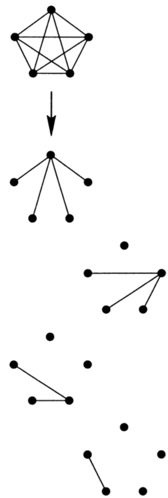
もう少しがんばって，グラフ理論でやってみよう．（基本的なグラフの概念はこの章の附録に書いておいた.）ちょっと考えてみれば，次の命題が定理 3 とまったく同じであることがわかる．

> **完全グラフ K_n を，あらゆる辺がただ 1 つのクリークに属すように，K_n とは異なる m 個のクリークに分割すれば，$m \geq n$ となる．**

実際，X を K_n の頂点集合に対応させ，集合 A_i をクリークの頂点集合に対応させれば，命題はまったく同じになる．

次の問題は，K_n を完全 2 部グラフに分解して，またあらゆる辺がそれらのグラフのちょうど 1 つに含まれるようにすることである．これをするのは易しい．頂点に $\{1, 2, \ldots, n\}$ と番号をつける．最初に，1 と他のすべての頂点とを結ぶ完全 2 部グラフをとる．すると，**スター**と呼ばれるグラフ $K_{1,n-1}$ が得られる．次に，2 と $3, \ldots, n$ を結ぶ．得られるのはスター $K_{1,n-2}$ である．これを続けていくと，K_n はスター

$K_{1,n-1}, K_{1,n-2}, \ldots, K_{1,1}$ に分解される．この分解は $n-1$ 個の完全 2 部グラフを使っている．もっとうまく，つまり，グラフの数をもっと減らせるだろうか？ 次のロン・グレアムとヘンリー・O・ポラックの結果が言っているように，答えはノーである．



4 つの完全 2 部グラフへの K_5 の分解．

定理 4． K_n **が完全 2 部グラフ** $H_1, \ldots, H_m$ **に分解されたなら，** $m \geq n-1$ **である．**

興味深いことに，エルデシュ–ド・ブリュインの定理とは違って，この結果には組合せ論的な証明が知られていない！ どれも何かしら線形代数を使っている．大体は同値である様々なアイデアの中から，ツヴァベリによる証明を見てみよう．おそらく一番見通しがよいものである．

■ **証明．** K_n の頂点集合を $\{1, \ldots, n\}$ とし，完全 2 部グラフ H_j, $j = 1, \ldots, m$ を定める頂点集合を L_j, R_j とする．各頂点 i に変数 x_i を与える．$H_1, \ldots, H_m$ が K_n を分解しているので，

$$\sum_{i<j} x_i x_j \quad = \quad \sum_{k=1}^{m} \Big(\sum_{a \in L_k} x_a \cdot \sum_{b \in R_k} x_b\Big) \qquad (1)$$

となる．ここで，定理が間違っている，つまり，$m < n-1$ であると仮定する．すると線形方程式系

$$\begin{aligned} x_1 + \cdots + x_n &= 0, \\ \sum_{a \in L_k} x_a &= 0 \qquad (k = 1, \ldots, m) \end{aligned}$$

は，変数の数より方程式の数が少ないことになり，それゆえ自明でない解 $c_1, \ldots, c_n$ を持つことになる．(1) から

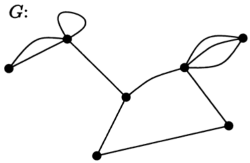
$$\sum_{i<j} c_i c_j \quad = \quad 0$$

となるが，これから

$$0 \;=\; (c_1 + \cdots + c_n)^2 \;=\; \sum_{i=1}^{n} c_i^2 + 2\sum_{i<j} c_i c_j \;=\; \sum_{i=1}^{n} c_i^2 \;>\; 0$$

が得られる．これは矛盾であり，証明が終わる． □

附録：基本的なグラフの概念

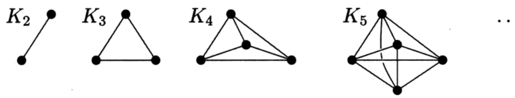


グラフ G は 7 つの頂点と 11 個の辺を持っている．ループが 1 つ，2 重辺が 1 つ，3 重辺が 1 つある．

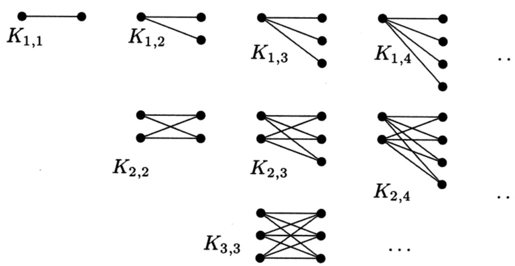
グラフは全数学の中でもっとも基本的な構造の 1 つである．また，多くの異なる表し方や具体化がある．抽象的には，**グラフ**とは，対 $G=(V,E)$ のことで，V が**頂点**の集合で，E が**辺**の集合であり，各辺 $e \in E$ は 2 つの頂点 $v,w \in V$ を「結んで」いる．ここでは，V と E が有限である，有限グラフだけを考えることにする．

普通は**単純グラフ**を扱う．そのとき，**ループ**，つまり両端が一致する辺や，**多重辺**，つまり両端が同じ集合になる辺を認めないことにする．グラフの頂点が**隣接する**とは，1 つの辺の両端の頂点になっているときに言い，頂点と辺が**接続している**とは，頂点がその辺の端点になっているときに言う．

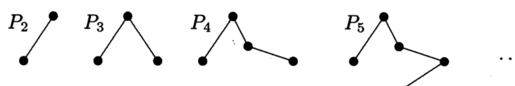
重要な（単純）グラフの小さな画廊をお目にかけよう．



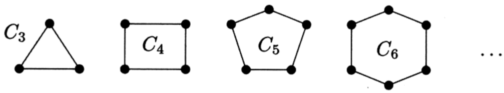
n 個の頂点と $\binom{n}{2}$ 個の辺からなる**完全グラフ** K_n.



$m+n$ 個の頂点と mn 個の辺を持つ**完全 2 部グラフ** $K_{m,n}$.

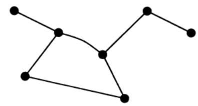


n 個の頂点を持つ**道** P_n.

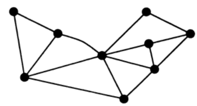


n 個の頂点を持つサイクル C_n.

2つのグラフ $G=(V,E)$ と $G'=(V',E')$ が**同型**であると考えられるのは，2つの全単射 $V \to V'$ と $E \to E'$ があって，辺とその端点との間の接続関係を保つときである．(2つの与えられたグラフが同型であるかどうかを決定する効果的なテストが存在するか，というのは主要な未解決問題である.) この同型の概念によって，5頂点上の完全グラフ K_5 などという言い方が許されることになる[4].



は次のグラフの部分グラフ.



$G'=(V',E')$ が $G=(V,E)$ の**部分グラフ**であるのは，$V' \subseteq V, E' \subseteq E$ であり，あらゆる辺 $e \in E'$ が G' と G で同じ端点を持つときである．さらに，G' の頂点を結ぶ G のすべての辺がまた G' の辺でもあるとき，G' は**誘導された部分グラフ**と言う．

グラフに関する多くの概念はまったく直観的なものである．たとえば，グラフ G が**連結**なのは，異なる2つのあらゆる頂点が G の道で結ばれるとき，またはこれと同値だが，G を2つの空でない部分グラフに分解し，その頂点集合に交わりがないようにはできないときである．

グラフの基本概念の復習を終えるに際して，もう少し用語を挙げておこう．G の**クリーク**とは完全部分グラフのことである．G の中の**独立集合**とは辺を持たない誘導された部分グラフ，つまり頂点集合の部分集合で，どの2頂点も G の辺では結ばれないもののことである．サイクルを含まないグラフを**森**と言う．連結な森を**木**と言う．最後に，グラフ $G=(V,E)$ が**2部**であるとは，ある完全2部グラフの部分グラフに同型なとき，つまり，その頂点集合を2つの独立集合の和 $V=V_1 \cup V_2$ として書くことができるときである．

参考文献

[1] N. G. ド・ブリュイン， P. エルデシュ：「ある組合せの問題」(*On a combinatorial problem*), Proc. Kon. Ned. Akad. Wetensch. **51** (1948), 1277-1279.

---

4 ［訳註］もちろん，5頂点上の完全グラフはすべて同型だということの反映として，ということ．

[2] H. S. M. コクセター：「共線的な点の問題」(*A problem of collinear points*), Amer. Math. Monthly **55** (1948), 26-28 （ケリーの証明を含む）.

[3] P. エルデシュ：「問題 4065 — 3 点共線性」(*Problem 4065 — Three point collinearity*), Amer. Math. Monthly **51** (1944), 169-171（ガライの証明を含む）.

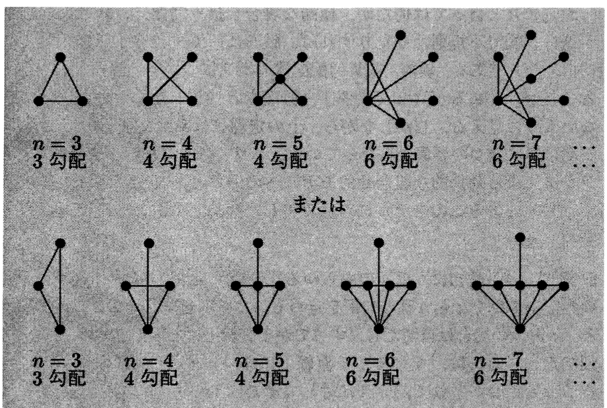
[4] R. L. グレアム, H. O. ポラック：「ループ・スウィッチングに対する名前付け問題」(*On the addressing problem for loop switching*), Bell System Tech. J. **50** (1971), 2495-2519.

[5] J. J. シルヴェスター：「数学の問題 11851」(*Mathematical Question 11851*), The Educational Times **46** (1893), 156.

[6] H. ツヴァベリ：「K_n の完全 2 部グラフへの分解について」(*On the decomposition of K_n into complete bipartite graphs*), J. Graph Theory **6** (1982), 493-494.

第9章　勾配問題

これから先を読む前に,「相対的に少ない数の」勾配を定める平面の点の配置という問題を考えてみて欲しい．このためにはもちろん，$n \geq 3$ 個の点がすべて 1 つの直線の上にあることはないと仮定する.「平面の中の直線」に関する第 8 章のエルデシュ–ド・ブリュインの定理を思い出せば，n 個の点は少なくとも n 個の異なる直線を定めたのだった．しかし，もちろん，これらの直線の多くが平行になって，同じ勾配を定めるかも知れない.



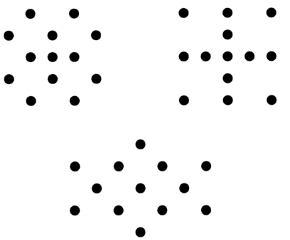
小さな n に対して少し実験してみると，多分ここに描いた 2 種類の系列が得られるだろう.

少ない数の勾配を持つ配置を見つける努力をしていけば，そのうち 1970

年にスコットがしたように，次の定理を予想できるかも知れない．

> **定理．もし平面上の $n \geq 3$ 個の点がある 1 つの直線上にはないとすれば，少なくとも $n-1$ 種の異なる勾配を定める．等号が成り立つのは，n が $n \geq 5$ で奇数のときだけである．**

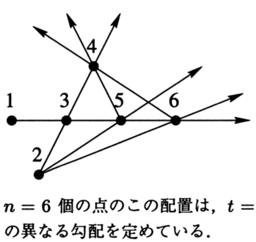
前ページの図は，配置例の 2 つの無限系列を初めの方だけ表わしたものだが，この例は定理が**最良**であること，つまり，どんな奇数の $n \geq 5$ に対しても，ちょうど $n-1$ 種の異なる勾配を定める n 個の点の配置が存在し，他の $n \geq 3$ に対してはちょうど n 種の異なる勾配を持つ配置が存在することを示している．



3 つの素敵な散在的な例，ジェイミスン–ヒルのカタログから．

しかしながら，上に描いた配置が唯一のものであるということは，とても言えない．たとえば，ジェイミスンとヒルは，配置の 4 つの無限の族を述べており，それぞれが $n-1$ 種の勾配しか定めない奇数 n 個の点の配置（「臨界勾配配置」）からなっている．さらに彼らは，無限の族には入れることができそうもない 102 もの「散在的」な例を挙げている．それらは計算機の広汎な利用によって探し出したものである．

お定まりと言っては何だが，極端な場合を扱う問題は，極端な配置が余りに多様で不規則だったりすれば，厳密に解くのは非常に難しいことになりがちである．実際，臨界勾配配置の構造について，言うことのできることが多くあるが（[2] を参照），分類などはまったく手の届く範囲にないように見える．しかしながら，上の定理には単純な証明が存在する．証明は主に 2 つの要素からなっている．エリ・グッドマンとリッキー・ポラックによる効果的な組合せ的モデルへの帰着と，1982 年のピーター・アンガーによるこのモデルにおける美しい議論とである．それで証明が完結する．



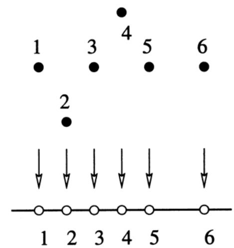
$n=6$ 個の点のこの配置は，$t=6$ 種の異なる勾配を定めている．

■ **証明．(1)** 最初に，平面のあらゆる「偶数」$n=2m$ $(m \geq 2)$ 個の点の集合が少なくとも n 種の勾配を定めることを示せば十分なことに注意する．$n=3$ の場合は自明だし，(すべてが 1 直線上にない) $n=2m+1 \geq 5$ 個の点に対しては，(すべてが 1 直線上にない) $n-1=2m$ 個の点からなる部分集合がとれて，それに対してすでに $n-1$ 種の勾配が定められている．

そこで，以下では，平面上の $n=2m$ 個の点の配置で，$t \geq 2$ 種の異

なる勾配を定めるものを考えることにする.

(2) 組合せ的モデルは，順列の周期的な列を構成することによって得られる．このために，配置の作る勾配のどれとも一致しないある方向から始めて，その方向への 1 次元射影の中に現れる順番に，点に $1, \ldots, n$ と番号をつける．つまり，順列 $\pi_0 = 123\cdots n$ が最初の方向に対する点の順序を表わすことになる.



これが最初の垂直方向で $\pi_0 = 123456$ を与える.

次に方向を反時計回りに回転させ，射影とその順列がどうなるかを見ていく．射影された点の順序が変わるのは，この方向が配置の勾配を通過する瞬間である.

しかし，変わり方はデタラメに起こるのでも勝手な仕方で起こるのでもない．180° の回転をすれば，順列の列

$$\pi_0 \to \pi_1 \to \pi_2 \to \cdots \to \pi_{t-1} \to \pi_t$$

が得られ，その列は以下のような特殊な性質を持っている.

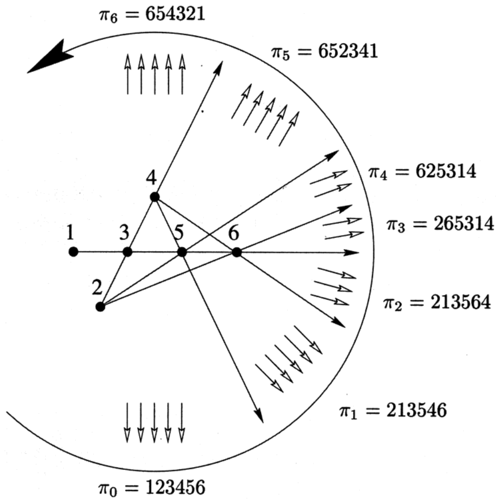
- 列は $\pi_0 = 123\cdots n$ で始まり，$\pi_t = n\cdots 321$ で終わる.
- 列の長さ t は点配置の勾配の数である.
- 列が進んでいくと，あらゆる対 $i < j$ は一度だけ入れ代わる．つまり，$\pi_0 = 123\cdots n$ から $\pi_t = n\cdots 321$ への道で，**増大**部分列だけが反転するのである.
- 列が 1 つ進むのは，(その点を通る方向を持つ 1 つ以上の直線に対応した) 1 つ以上の交わらない増大部分列の反転の形で起こる.

点配置の周りを回り続ければ，この列が，両方向に無限で周期的な順列の列

$$\to \pi_{-1} \to \pi_0 \to \cdots \to \pi_t \to \pi_{t+1} \to \cdots \to \pi_{2t} \to \cdots$$

の一部になっていると見ることができるようになる．ここで，すべての $i \in \mathbb{Z}$ に対して π_{i+t} は π_i を反転したものであり，また $\pi_{i+2t} = \pi_i$ となっている.

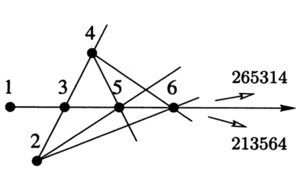
上の性質（と $t \geq 2$）を満たす列はすべて，長さが $t \geq n$ であることを示すことにしよう.



上の簡単な例で得られる順列.

(3) 証明のポイントは，順列をそれぞれ同じ大きさ $m = \frac{n}{2}$ の「左半分」と「右半分」に分け，数字が左半分と右半分の間の想像上の**境界線**を横切る回数を数えることである．

$\pi_i \to \pi_{i+1}$ を**横断移行**と呼ぶのは，それが反転する部分列の 1 つが境界線の両側の数字を含んでいるときとする．横断移行が**位数** d であるとは，$2d$ 個の数字が境界を横切るとき，つまり，横断している部分列が一方にちょうど d 個の数字を持ち，他方に少なくとも d 個の数字を持っているときである．上の例では



横断移行.

$$\pi_2 \;=\; 2\underline{13{:}56}4 \longrightarrow 2\overline{65{:}31}4 \;=\; \pi_3$$

は位数 $d = 2$ の横断移行であり（これは「:」で印した境界を横断する $1, 3, 5, 6$ を動かしている），

$$65\underline{2{:}34}1 \longrightarrow 65\overline{4{:}32}1$$

は位数 $d_2 = 1$ の横断移行である．またこの例での

$$6\underline{25}{:}3\underline{14} \longrightarrow 6\overline{52}{:}3\overline{41}$$

は横断移行ではない．

列 $\pi_0 \to \pi_1 \to \cdots \to \pi_t$ を進んでいくとき，数字 $1, 2, \ldots, n$ は少なくとも 1 回境界線を横断しなければならない．c 回の横断移行の位数を $d_1, \ldots, d_c$ と書けば，

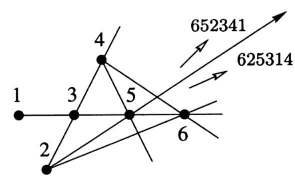
$$\sum_{i=1}^{c} 2d_i \;=\; \#\{\text{ 境界線を横断する数字 }\} \;\geq\; n$$

となる．このことからまた．少なくとも 2 回の横断移行があることがわかる．というのは，$2d_i = n$ である横断移行が起こるのは，すべての点が 1 直線上にあるとき，つまり $t = 1$ のときだけだからである．幾何的には，横断移行は，それぞれの側に m 個より少ない点があるような配置の直線の方向に対応している．

(4) 接触移行とは，中央の境界線に隣りあったある部分列を反転させるが，境界線を横断しないような移行のこととする．たとえば，

$$\pi_4 \;=\; 6\underline{25}{:}3\underline{14} \longrightarrow 6\overline{52}{:}3\overline{41} \;=\; \pi_5$$

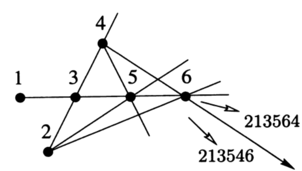
は接触移行である．幾何的には，接触移行は，一方の側にはちょうど m 個の点があり，それゆえもう一方の側には高々 $m-2$ 個の点しかないような配置の直線の勾配に対応している．



接触移行．

接触移行でも横断移行でもないものを**通常移行**と言う．この例としては

$$\pi_1 \;=\; 213{:}5\underline{46} \longrightarrow 213{:}5\overline{64} \;=\; \pi_2$$



通常移行．

がある．あらゆる移行は，接触 (touching) か横断 (crossing) か通常 (ordinary) のどれかであり，移行のタイプを表わすのに T, C, O という文字を使うことができる．位数 d の横断移行を $C(d)$ と表わすと，上の例に対しては

$$\pi_0 \xrightarrow{T} \pi_1 \xrightarrow{O} \pi_2 \xrightarrow{C(2)} \pi_3 \xrightarrow{O} \pi_4 \xrightarrow{T} \pi_5 \xrightarrow{C(1)} \pi_6$$

が得られ，この列をさらに短く $T, O, C(2), O, T, C(1)$ と記録することもできる．

(5) 証明を完結させるには次の2つの事実が必要となる．

> **どの2つの横断移行の間にも，少なくとも1つの接触移行が存在する．**
>
> **位数 d の横断移行と次の接触移行の間には，少なくとも $d-1$ 個の通常移行が存在する．**

実際，位数 d の横断移行のあとでは，境界線は長さが $2d$ の対称な減小部分列の中にあることになり，境界線の両側にはその列の d 個の数字があるようになる．次の横断移行のときには，中心の境界線は少なくとも2の長さの増大部分列の中に入っていなければならない．しかし，境界線がある増大部分列に入っているかどうかに影響を与えるのは，接触移行だけである．このことにより最初の事実が得られる．第2の事実に対しては，(ある増大部分列を反転させる) 通常移行では，減小 $2d$ 列はそれぞれの側で1数字分しか短くなることができないことを注意する．そして，減小部分列が少なくとも4つの数字を含んでいる限り，接触移行は起こり得ない．このことにより，第2の事実が得られる．

もし，同じ初期射影から始めて，時計回りの回転によって順列を作ったなら，順列を反転したものが得られる．そのため，記録した列は，上の第2の事実を反対にしたもの，つまり

> **接触移行と次の位数 d の横断移行の間には，少なくとも $d-1$ 個の通常移行が存在しなければならない，**

もまた満たさなければならない．

(6) (2) で導かれた無限の順列の T-O-C パターンは，長さ t の列 $\pi_0 \longrightarrow \cdots \longrightarrow \pi_t$ の T-O-C パターンを何度も繰り返すことによって得られる．(5) の事実と合わせれば，無限の移行列の中に，位数 d の横断移行はそれぞれ，長さ $1+(d-1)+1+(d-1)=2d$ の

$$T, \underbrace{O, O, \ldots, O,}_{\geq\, d-1} C(d), \underbrace{O, O, \ldots, O}_{\geq\, d-1} \qquad (*)$$

というタイプの T-O-C パターンの中に埋め込まれることがわかる．

無限列の中から，ある接触移行で始まる長さ t の有限の区間を考えることができる．この区間は $(*)$ のタイプの部分列に，余分な T をいく

つか足したものからなる．このことから，その長さ t は

$$t \;\geq\; \sum_{i=1}^{c} 2d_i \;\geq\; n$$

を満たさなければならず，証明が終わる． □

参考文献

[1] J. E. グッドマン，R. ポラック：「幾何学における問題の組合せ的な見方」(*A combinatorial perspective on some problems in geometry*), Congressus Numerantium **32** (1981), 383-394.

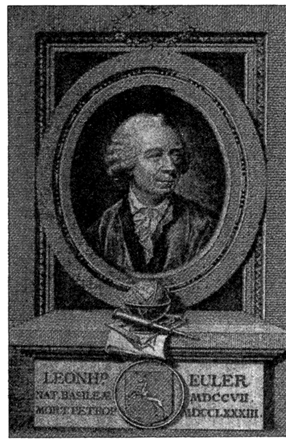
[2] R. E. ジェイミスン，D. ヒル：「臨界勾配配置のカタログ」(*A catalogue of slope-critical configurations*), Congressus Numerantium **40** (1983), 101-125.

[3] P. R. スコット：「n 個の点によって定まる方向の集合について」(*On the sets of directions determined by n points*), Amer. Math. Monthly **77** (1970), 502-505.

[4] P. アンガー：「$2N$ 個の非共線的な点は少なくとも $2N$ 個の方向を定める」($2N$ *noncollinear points determine at least* $2N$ *directions*), J. Combinatorial Theory Ser. A **33** (1982), 343-347.

第10章　オイラーの公式の3つの応用

グラフが**平面グラフ**であるとは，辺が交わることなく平面 $\mathbb{R}^2$（または，同値だが，2次元球面 S^2）上に描くことができることである．これから**平面**グラフについて述べるときには，このような描き方がすでに与えられており，固定されているものと考える．そのような図は平面または球面を，(有界でない) 外部領域も含めて有限個の連結領域に分割する．それらは**面**と呼ばれる．オイラーの公式は，頂点と辺と面の数の間の美しい関係を表わしており，どんな平面グラフに対しても成り立っている．オイラーがこの結果を初めて述べたのは，友人であるゴールドバッハへの1750年の手紙の中であったが，当時彼は完全な証明は持っていなかった．オイラーの公式の多くの証明の中から，帰納法を使わないエレガントで「自己双対的な」証明を述べようと思う．その証明は1847年のフォン・シュタウトの本『位置の幾何学』にまで遡ることのできるものである．



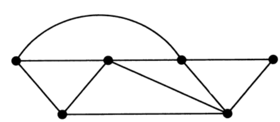
レオンハルト・オイラー

オイラーの公式． G が連結平面グラフで，n 個の頂点，e 個の辺，f 個の面を持てば，次の関係式が成り立つ．

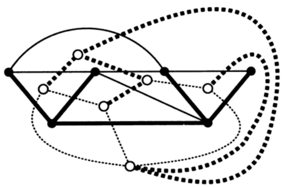
$$n - e + f = 2.$$

■ **証明．** $T \subseteq E$ を，G を**全域木**，つまり G のすべての頂点を結ぶ極小の部分グラフの，辺の集合とする．極小性の仮定から，このグラフはサイクルを含まない．

ここで，G の**双対グラフ** G^* が必要になる．これを作るには，G の各面の内部に頂点をとり，G^* の2つの頂点に対して，対応する（G の）面に共通の境界辺があるとき，その2頂点を結んで（G^* の）辺とする．



平面グラフ G: $n = 6$, $e = 10$, $f = 6$.

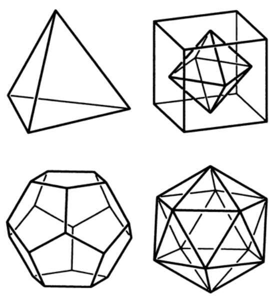


G と G^* における双対な全域木.

もし境界辺が複数あるなら，双対グラフでも複数の辺で結ぶことになる．（こうして，元のグラフ G が単純グラフであっても，G^* は多重辺を持つ可能性がある.）

双対グラフの中で，$E \backslash T$ の辺に対応する辺の集合 $T^* \subseteq E^*$ を考える．T がサイクルを持たないので，T^* の辺はすべての面を結んでいる．しかし，T^* もまたサイクルを含まない．もしそうでないなら，サイクルの内部にある G のある頂点が，外部にある頂点から分離されてしまうからである（これは起こり得ない．なぜなら，T は全域木であり，T と T^* の辺は交わらないからである）．こうして，T^* は G^* に対して，全域木になっている．

木に対しては，頂点の数は辺の数より 1 だけ大きい．このことを見るために，1 つの頂点を根として選び，すべての辺を「根から離れる」ように向きをつける．各辺とその行き先の頂点とを対応させることによって，根でない頂点と辺との間の全単射が得られる．木 T に対しては $n = e_T + 1$ が得られ，木 T^* に対しては $f = e_{T^*} + 1$ が得られる．2 つの式を足せば，$n + f = (e_T + 1) + (e_{T^*} + 1) = e + 2$ が得られる．　□



5 つのプラトンの立体.

このように，オイラーの公式は**幾何的トポロジー**の状況から強力な**数値的**な結論を生み出す．有限グラフ G の頂点，辺，面の数は，それが平面もしくは球面上に描かれている，**または**，描くことが**できる**のであれば，$n - e + f = 2$ を満たすのである．

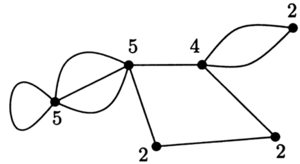
多くのよく知られた古典的な結果をオイラーの公式から導くことができる．そのようなものには，凸の正多面体（プラトンの立体）の分類，K_5 と $K_{3,3}$ が平面グラフでないという事実（以下を参照），あらゆる平面的な地図を，隣り合った国を同じ色にしないように，高々5 つの色で塗り分けることができるという 5 色定理がある．しかしこれに対しては，オイラーの公式を使う必要すらない，ずっとよい証明がある．このことについては第 27 章を参照すること．

この章には，オイラーの公式が核になっている，上に挙げた以外の 3 つの美しい証明を集めてみた．最初の 2 つは，シルヴェスター–ガライの定理と 2 色の点配置に関する定理の証明で，基本的なグラフのパラメータの間の算術的な関係式とオイラーの公式を上手に組み合わせて使うのである．まず，これらのパラメータを考えよう．

頂点の**次数**は，その頂点を端点とする辺の個数である．ループの場合

は 2 重に数えることとする．n_i をグラフ G における次数 i の頂点の数とする．次数によって頂点を数えると，

$$n = n_0 + n_1 + n_2 + n_3 + \cdots \tag{1}$$



ここでは次数は各頂点の近くに書かれている．与えられた次数を持つ頂点を数えると，$n_2 = 3$, $n_3 = 0$, $n_4 = 1$, $n_5 = 2$ となる．

となる．一方，あらゆる辺は 2 つの端点を持つので，すべての次数の和には 2 重に数えられるから，

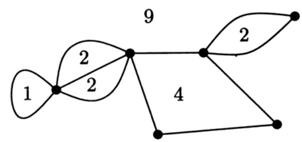
$$2e = n_1 + 2n_2 + 3n_3 + 4n_4 + \cdots \tag{2}$$

が得られる．この恒等式は，辺の端点を 2 通りの方法で数えたもの，つまり，辺–頂点接続関係と解釈することができる．したがって，頂点の**平均次数** $\overline{d}$ は

$$\overline{d} = \frac{2e}{n}$$

となる．

次に，平面グラフの面をその辺の数に従って数えよう．k **面**とは，k 個の辺で囲まれた面のことである（辺はその両側で面の境界になるので，同じ領域を 2 度数えることになる！）．f_k を k 面の数とする．すべての面を数えると，



辺の数が各領域の中に書かれている．与えられた辺の数を持つ面を数えると，$f_1 = 1$, $f_2 = 3$, $f_4 = 1$, $f_9 = 1$, その他は $f_i = 0$ となる．

$$f = f_1 + f_2 + f_3 + f_4 + \cdots \tag{3}$$

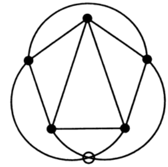
が得られる．辺を，それを辺に持つ面に従って数えると，

$$2e = f_1 + 2f_2 + 3f_3 + 4f_4 + \cdots \tag{4}$$

が得られる．前と同じように，辺–面結合を 2 重に数えたものと解釈することができる．面の，平均の辺の数は

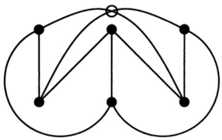
$$\overline{f} = \frac{2e}{f}$$

によって与えられることに注意する．



交差が 1 つになるように描いた K_5.

オイラーの公式と合わせると，上のことからすぐに，完全グラフ K_5 と完全 2 部グラフ $K_{3,3}$ が平面グラフでないことが導かれる．K_5 が平面に描けたと仮定して計算すると，$n = 5$, $e = \binom{5}{2} = 10$ となり，だから $f = e + 2 - n = 7$ かつ $\overline{f} = \frac{2e}{f} = \frac{20}{7} < 3$ となる．しかし，平均の辺の数が 3 より小さければ，埋め込みには高々2 つの辺を持つ面がある



交差が 1 つになるように描いた $K_{3,3}$.

ことになるが，それはあり得ない．

同じように，$K_{3,3}$ に対しては，$n=6$, $e=9$, $f=e+2-n=5$ となり，$\overline{f}=\frac{2e}{f}=\frac{18}{5}<4$ が得られるが，これはあり得ない．というのは，$K_{3,3}$ は単純グラフかつ 2 部グラフなので，すべてのサイクルの長さは少なくとも 4 だからである．

f_i に対する等式 (3) と (4) が n_i に対する等式 (1) と (2) にこんなに似ているのは，もちろん偶然ではない．上で説明した双対グラフの構成 $G \to G^*$ によって，それらの式は互いに移り合うのである．

2 重に数えることで得られる恒等式から，オイラーの公式の以下のような重要な「局所的」な結果が得られる．

命題. G **を空でない単純な平面グラフとする．そのとき，以下のことが成り立つ．**

(A) G **は高々 5 次の頂点を持つ．**

(B) G **の辺の数は高々** $3n-6$ **である．**

(C) **もし** G **の辺が 2 色で塗られていれば，**G **の頂点で，その周りで順に見ると辺の色が高々2 回しか変らないようなものがある．**

■ **証明.** この 3 つの主張の証明では，それぞれ，G が連結グラフであると仮定してもよい．

(A) あらゆる面は少なくとも 3 つの辺を持つ（G が単純グラフだから）ので，(3) と (4) から

$$\begin{aligned} f &= f_3 + f_4 + f_5 + \cdots \\ 2e &= 3f_3 + 4f_4 + 5f_5 + \cdots \end{aligned}$$

が得られ，$2e-3f \geq 0$ となる．

ここで，もし頂点の次数がそれぞれ少なくとも 6 であれば，(1) と (2) から，

$$\begin{aligned} n &= n_6 + n_7 + n_8 + \cdots \\ 2e &= 6n_6 + 7n_7 + 8n_8 + \cdots \end{aligned}$$

が得られ，$2e-6n \geq 0$ となる．

2 つの不等式を合わせると，

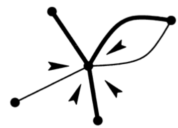
$$6(e-n-f) \;=\; (2e-6n)+2(2e-3f) \;\geq\; 0$$

が，つまり，$e \geq n + f$ が得られ，これはオイラーの公式に矛盾する．

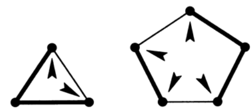
(B) (A) の証明の最初のステップとして $2e - 3f \geq 0$ が得られていたので，オイラーの公式から，

$$3n - 6 \;=\; 3e - 3f \;\geq\; e$$

となる．



矢印は色が変わる角を指している．



(C) c を色が変わる角の数とする．主張が誤りだと仮定すると，$c \geq 4n$ 回色が変わることになる．というのも，あらゆる頂点で色が変わるのは偶数回だからである．そこで，$2k$ または $2k+1$ 個の辺を持つ面ではそのような角は高々 $2k$ 個であり，また (3) と (4) を使うと，

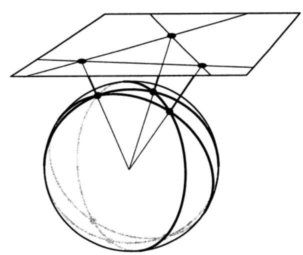
$$\begin{aligned}
4n \;\leq\; c \;&\leq\; 2f_3 + 4f_4 + 4f_5 + 6f_6 + 6f_7 + 8f_8 + \cdots \\
&\leq\; 2f_3 + 4f_4 + 6f_5 + 8f_6 + 10f_7 + \cdots \\
&=\; 2(3f_3 + 4f_4 + 5f_5 + 6f_6 + 7f_7 + \cdots) \\
&\quad\; -4(f_3 + f_4 + f_5 + f_6 + f_7 + \cdots) \\
&=\; 4e - 4f
\end{aligned}$$

が得られる．それゆえ，$e \geq n + f$ となるが，これはまたオイラーの公式に矛盾する． □

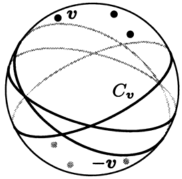
1. シルヴェスター–ガライの定理をもう一度

命題の (A) がシルヴェスター–ガライの定理（第 8 章参照）の驚くほど簡単な証明を与えることを最初に注意したのは，ノーマン・スティーンロッドであるらしい．

> **シルヴェスター–ガライの定理．平面上に，すべては 1 直線上にない $n \geq 3$ 個の点の集合が与えられたなら，2 点だけを含む直線が常に存在する．**



■ **証明．**（オイラーを経由したシルヴェスター–ガライ） 図に示したように，$\mathbb{R}^2$ を $\mathbb{R}^3$ の中の単位球面 S^2 の近くに埋め込むと，あらゆる $\mathbb{R}^2$ の点は S^2 の 1 対の対蹠点に対応し，$\mathbb{R}^2$ の直線は S^2 の大円に対応する．するとシルヴェスター–ガライの定理は次のようになる．



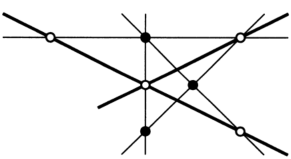
球面上に，すべては 1 つの大円の上にない対蹠点の $n \geq 3$ 対の集合が与えられたなら，2 対の対蹠点だけを含む大円が常に存在する．

ここで問題を，各対蹠点の対を球面上の対応する大円で置き換えることによって，双対化する．つまり，点 $\pm\boldsymbol{v} \in S^2$ の代わりに，$C_{\boldsymbol{v}} = \{\boldsymbol{x} \in S^2 : \langle \boldsymbol{x}, \boldsymbol{v} \rangle = 0\}$ で与えられる大円を考える．($\boldsymbol{v}$ を球面の北極と考えたら，この $C_{\boldsymbol{v}}$ は赤道である.) すると，シルヴェスター–ガライの定理は次のことを証明することになる．

S^2 上に，すべてがある 1 点を通るわけではない，$n \geq 3$ 個の大円の集合が与えられたなら，2 つの大円だけが通る点が常に存在する．

しかし，これらの大円によって，S^2 上に単純平面グラフが得られる．2 つの大円の交点が頂点であり，それで大円を辺に切り分けるのである．すべての頂点の次数は偶数であり，作り方から少なくとも 4 以上である．すると，命題の (A) から 4 次の頂点が存在することになる．できてしまった !! □

2. 単色の直線



次のシルヴェスター–ガライの定理の「カラー」版はドン・チェイカリアンによる．

定理． **平面上に，すべてが 1 直線上にはない，「黒」と「白」の有限個の点が置かれていると，常に「単色」の直線，つまり，1 つの色の点を 2 つ以上含み他の色の点を含まない直線が存在する．**

■ **証明．** シルヴェスター–ガライの定理については，問題を単位球面に移し，そこで双対化した．それで，次のことを証明することにする．

すべてがある 1 点を通っているわけではない，有限個の「黒」と「白」の大円が与えられたなら，白の大円だけの上にあるか，または黒の大円だけの上にある交点が常に存在する．

さて,（肯定的な）解答は命題の (C) から明らかである．というのは，異なる色の大円が交わるあらゆる頂点において，符号の変わる角が常に少なくとも 4 つ存在するからである． □

3. ピックの定理

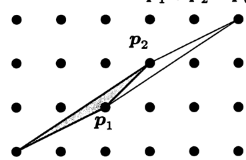
1899 年以来知られている**ピックの定理**は，それ自身美しくまた驚くべき結果であるが，オイラーの公式の「古典的」な帰結の 1 つでもある．以下のために，凸な格子多角形 $P \subseteq \mathbb{R}^2$ を**基本多角形**と呼ぶのは，頂点がすべて整数点で，それ以外には整数点を含まないときとする．

補題． **あらゆる基本三角形** $\Delta = \mathrm{conv}\{\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2\} \subseteq \mathbb{R}^2$ **の面積は** $A(\Delta) = \frac{1}{2}$ **である．**

■ **証明．** $\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_1 + \boldsymbol{p}_2 - \boldsymbol{p}_0$ に角を持つ平行四辺形 P と格子 $\mathbb{Z}^2$ はともに，写像

$$\sigma : \boldsymbol{x} \longmapsto \boldsymbol{p}_1 + \boldsymbol{p}_2 - \boldsymbol{x}$$

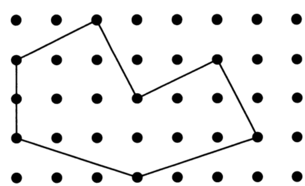
に関して対称である．この写像は，$\boldsymbol{p}_1$ と $\boldsymbol{p}_2$ を結ぶ線分の中点に関する点対称である．こうして，平行四辺形 $P = \Delta \cup \sigma(\Delta)$ もまた基本多角形であり，それに整数的な平行移動をすると平面のタイル張りが得られる．それゆえ，$\{\boldsymbol{p}_1 - \boldsymbol{p}_0, \boldsymbol{p}_2 - \boldsymbol{p}_0\}$ は格子 $\mathbb{Z}^2$ の基底であり，その行列式は 1 であり，P の面積は 1 であり，Δ の面積は $\frac{1}{2}$ である．(これらの用語の説明については以下の箱を参照のこと．) □



定理．（ピックの定理）　整数点を頂点とする，（必ずしも凸とは限らない）多角形 $Q \subseteq \mathbb{R}^2$ **の面積は**

$$A(Q) = n_{int} + \frac{1}{2} n_{bd} - 1$$

で与えられる．ここで，n_{int} **と** n_{bd} **はそれぞれ，**Q **の内部と境界上にある整数点の個数である．**



$n_{int} = 11$，$n_{bd} = 8$ だから $A = 14$.

■ **証明．** そのような多角形 Q は，内部の n_{int} 個の格子点と境界上の n_{bd} 個の格子点を使って三角形分割することができる．(このことはあまり明らかなわけではない．とくに Q を凸と仮定しないときはそうだが，

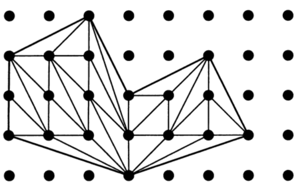
格子基底

$\mathbb{Z}^2$ の **基底**とは，1 次独立なベクトル $\boldsymbol{e}_1, \boldsymbol{e}_2$ の対で，

$$\mathbb{Z}^2 = \{\lambda_1 \boldsymbol{e}_1 + \lambda_2 \boldsymbol{e}_2 : \lambda_1, \lambda_2 \in \mathbb{Z}\}$$

を満たすもののことである．$\boldsymbol{e}_1 = \binom{a}{b}$, $\boldsymbol{e}_2 = \binom{c}{d}$ とおくと，$\boldsymbol{e}_1$ と $\boldsymbol{e}_2$ で張られる平行四辺形の面積は $A(\boldsymbol{e}_1, \boldsymbol{e}_2) = |\det(\boldsymbol{e}_1, \boldsymbol{e}_2)| = |\det \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)|$ で与えられる．もし $\boldsymbol{f}_1 = \binom{r}{s}$ と $\boldsymbol{f}_2 = \binom{t}{u}$ が別の基底であれば，可逆な $\mathbb{Z}$ 行列 Q が存在して，$\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) Q$ を満たす．$QQ^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ であり，行列式は整数だから，$|\det Q| = 1$ であり，$|\det(\boldsymbol{f}_1, \boldsymbol{f}_2)| = |\det(\boldsymbol{e}_1, \boldsymbol{e}_2)|$ となる．したがって，すべての基底平行四辺形は同じ面積 1 となる．それは，$A\left(\binom{1}{0}, \binom{0}{1}\right) = 1$ だからである．

第 28 章で美術館問題に関して使われる議論によって証明することができる.)



ここで，三角形分割を平面グラフとして説明することができ，それが平面を，有界でない 1 つの面と，面積が $\frac{1}{2}$ の $f-1$ 個の三角形に分割していると考えるのである．すると，

$$A(Q) = \frac{1}{2}(f-1)$$

となる．三角形は 3 つの辺を持ち，e_{int} 個の内部の辺は 2 つの三角形の境界となり，e_{bd} 個の境界の辺はそれぞれ 1 つの三角形にしか現れない．それで，$3(f-1) = 2e_{int} + e_{bd}$ となり，$f = 2(e-f) - e_{bd} + 3$ となる．また，境界上の頂点の数と辺の数は等しい，つまり $e_{bd} = n_{bd}$ である．この 2 つの事実とオイラーの公式から

$$\begin{aligned} f &= 2(e-f) - e_{bd} + 3 \\ &= 2(n-2) - n_{bd} + 3 \;=\; 2n_{int} + n_{bd} - 1 \end{aligned}$$

が得られ，

$$A(Q) \ = \ \tfrac{1}{2}(f-1) \ = \ n_{int} + \tfrac{1}{2}n_{bd} - 1$$

が得られる. □

参考文献

[1] G. D. チェイカリアン：「共線的な点に関するシルヴェスターの定理とその類似」(*Sylvester's problem on collinear points and a relative*), Amer. Math. Monthly **77** (1970), 164-167.

[2] G. ピック：「数論のための幾何」(*Geometrisches zur Zahlenlehre*), Sitzungsberichte Lotos (Prag), Natur-med. Verein für Böhmen **19** (1899), 311-319.

[3] G. K. C. フォン・シュタウト：『位置の幾何学』(*Geometrie der Lage*), Verlag der Fr. Korn'schen Buchhandlung, Nürnberg 1847.

[4] N. E. スティーンロッド：「解答 4065/編集ノート」(*Solution* 4065/ *Editorial Note*), Amer. Math. Monthly **51** (1944), 170-171.

第11章　コーシーの剛性定理

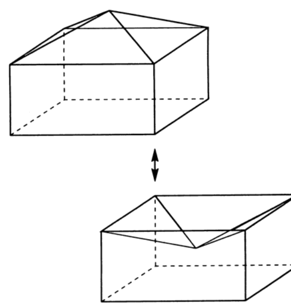
（とくに前章の命題の (C) のように）オイラーの公式を使って示される結果の中でも有名なものに，3 次元多面体に対するコーシーの剛性定理がある．

以下で用いる合同や組合せ同値の概念については，ヒルベルトの第3問題の章における多角形や多面体に関する附録（64 ページ）を参照のこと．



オーギュスタン・コーシー

定理. 2 つの 3 次元の凸多面体 P と P' が組合せ同値で，対応する面が合同であったとすれば，隣り合う面の対応する対の間の角もまた等しい（また，P と P' は合同である）.



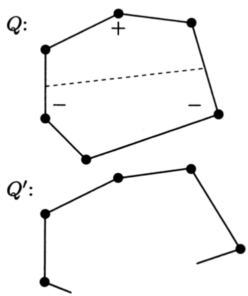
余白の図は，対応する面が合同な，組合せ同値な 2 つの 3 次元多面体を示している．それらは合同ではなく，凸であるのは一方だけである．つまり，凸であるという仮定はコーシーの定理にとって本質的なのである！

■ **証明.** 以下は本質的にはコーシーの元々の証明である．合同な面を持つ 2 つの凸多面体 P と P' が与えられているとする．P の辺に次のように色を塗る．ある辺が黒（または「正」）であるのを，それに隣り合う 2 つの面の間の対応する内角が P でよりも P' での方が大きいときとする．また，白（または「負」）であるのを，対応する角が P でよりも P' での方が小さいときとする．

P の黒と白の辺は P の表面に 2 色平面グラフを作り，(**0** が P の内部にあるとし）半径方向の射影によって球面 S^2 上の 2 色グラフに写すことができる．P と P' の対応する面角で等しくないものがあるときに

は，このグラフは空でなくなる．前章の命題 (C) から，ある頂点 p があって，その点に少なくとも 1 つの黒か白かの辺がつながっていて，(点の周りで順に数えて）高々2 回の黒白の辺の交替が起こっているようなものがある．

ここで，この頂点 p を中心とする（半径 ε の）小さな球面 S_ε と P と交わらせ，対応する頂点 p' を中心とする同じ半径 ε の球面 S'_ε と P' と交わらせる．S_ε と S'_ε の上に凸の球面多角形 Q と Q' を見つけることができ，対応する弧の長さは同じになっている．というのは，P と P' の面は合同で，半径も同じにとったからである．

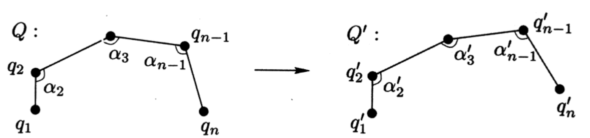


ここで，Q の角に，対応する Q' の角が大きいとき + の印をつけ，対応する Q' の角が小さいとき − の印をつける．つまり，Q から Q' に移るとき，+ の角は「開き」，− の角は「閉じ」る．このとき，すべての辺の長さと印のない角は変わらない．

p の選び方から，+ か − のどちらかの印は必ずあって，頂点の回りに高々2 回の +/− の交替があることがわかっている．もし 1 つの型の印しか現れなければ，1 つの辺の長さが変わってしまうことを示すことによって，下の補題から直接に矛盾を導く．両方の型の印が現れれば，(印の変化は 2 回しか起こらないので）ある 2 つの辺の中点を結ぶ直線で，+ の印と − の印を分ける「分離直線」があることになる．このときも下の補題から矛盾が得られる．なぜなら，この分離直線も，Q でのものが Q' でのものより，長くも短くもなれないからである．　□

コーシーのアーム補題．

Q と Q' が凸の（平面もしくは球面）n 角形で，図のように名前がついているとする．

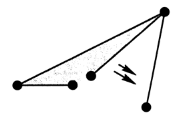


$1 \leq i \leq n-1$ に対する対応する辺の長さに関して $\overline{q_i q_{i+1}} = \overline{q'_i q'_{i+1}}$ となっていて，$2 \leq i \leq n-1$ に対する対応する角の大きさに関して $\alpha_i \leq \alpha'_i$ となっていたとすれば，「残りの」辺の長さは

$$\overline{q_1 q_n} \;\le\; \overline{q'_1 q'_n}$$

となる．等号が成り立つのは，すべての i に対して $\alpha_i = \alpha'_i$ であるとき，かつそのときに限る．

興味深いことだが，コーシー自身による補題の証明は，間違っていた．辺の長さを変えないで角を開く連続的な運動が凸性を破壊することがあり得るのである．図を参照のこと！　一方，ここで与える補題と証明はともに，I. J. シェーンベルクから S. K. ザレンバへの手紙からとったものだが，平面多角形と球面多角形の双方に対して有効である．



■ **証明.** n に関する帰納法を使う．$n = 3$ の場合は易しい．三角形において，固定された長さ a と b の 2 辺の間の角 γ を大きくすれば，対辺の長さ c も大きくなる．解析的には，これは平面の場合は余弦定理

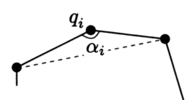
$$c^2 \;=\; a^2 + b^2 - 2ab\cos\gamma$$

から，そして球面の場合には球面三角法の類似の結果

$$\cos c \;=\; \cos a \cos b + \sin a \sin b \cos\gamma$$

から得られる．ここで，a, b, c は半径 1 の球面上で測ったもので，値は区間 $[0, \pi]$ にある．

ここで，$n \ge 4$ とする．どれかの $i \in \{2, \ldots, n-1\}$ に対して $\alpha_i = \alpha'_i$ だったなら，q_{i-1} から q_{i+1} へと，q'_{i-1} から q'_{i+1} への対角線を引くと $\overline{q_{i-1}q_{i+1}} = \overline{q'_{i-1}q'_{i+1}}$ となり，だから，対応する頂点に近道をつけることで，帰納法を使うことができる． こうして，$2 \le i \le n-1$ に対して $\alpha_i < \alpha'_i$ であると仮定してよい．

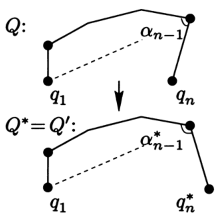


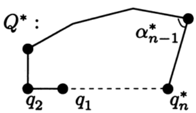
今度は，Q から新しい多角形 Q^* を作るのだが，Q^* が凸であることを保つように，α_{n-1} を可能な限り最大の角 $\alpha^*_{n-1} \le \alpha'_{n-1}$ で置き換える．このために，q_n を q^*_n で置き換えて，Q の他の辺の長さや角は変えないでおく．

もし実際に，Q^* が凸であるように $\alpha^*_{n-1} = \alpha'_{n-1}$ と選ぶことができたなら，第 1 段階の $n = 3$ の場合と上の第 2 段階の帰納法を使って，$\overline{q_1 q_n} < \overline{q_1 q^*_n} \le \overline{q'_1 q'_n}$ が得られる．

もしそうならないようなら，

$$\overline{q_1 q^*_n} \;>\; \overline{q_1 q_n} \tag{1}$$





となるような自明でない動かし方をして，3 点 q_2, q_1, q^*_n が 1 直線上に並ぶ，つまり，

$$\overline{q_2 q_1} + \overline{q_1 q^*_n} \;=\; \overline{q_2 q^*_n} \tag{2}$$

となる場合を「じっくり」考えることにする．今度はこの Q^* と Q' を比べて，n に関する帰納法を使うと

$$\overline{q_2 q^*_n} \;\leq\; \overline{q'_2 q'_n} \tag{3}$$

が得られる（頂点 q_1 と q'_1 は無視する）．こうして，

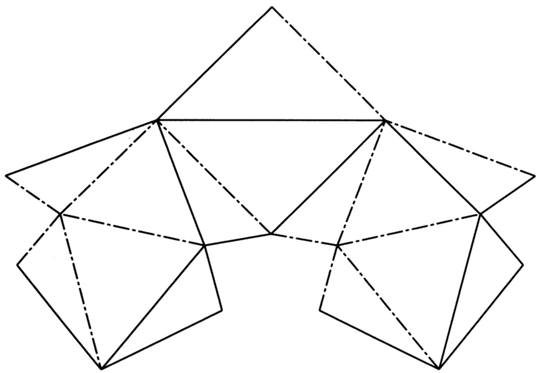
$$\overline{q'_1 q'_n} \;\overset{(*)}{\geq}\; \overline{q'_2 q'_n} - \overline{q'_1 q'_2} \;\overset{(3)}{\geq}\; \overline{q_2 q^*_n} - \overline{q_1 q_2} \;\overset{(2)}{=}\; \overline{q_1 q^*_n} \;\overset{(1)}{>}\; \overline{q_1 q_n}$$

が得られる．ここで，(∗) は単なる三角不等式で，他の関係式はすべてすでに導いたものである．　□

コーシーの定理が凸でない多面体に対しては成り立たないことを示す例をすでに見ている．この例の特徴はもちろん，1 つの多面体をもう 1 つの多面体に不連続的に「撥ね返す」とき，2 面角は「跳ぶ」が，面は合同のままということである．そこでさらに，次の問題を考えることができる．

> **凸でない多面体のうちには，面を平らで合同に保ったまま「連続的な変形」をすることが可能なものがあるだろうか？**

凸であろうとなかろうと，三角形分割されている曲面なら，そのような運動は許されないものと予想されていた．だから，1977 年に，コーシーの仕事から 160 年以上も経ってから，ロバート・コンリーが反例を示したことは，まったくの驚きだったのである．その反例は，$\mathbb{R}^3$ に（自己交差もなく）埋め込まれた閉じた三角形分割された球面で，すべての辺の長さを保ったまま，だから三角形の面が合同なままの連続的な運動（ジャバラ運動）で動かしても元に戻るようなものであった．



クラウス・シュテッフェンによって構成された，ジャバラ運動を持つ曲面の美しい例．この紙の「切り取り」モデルで，破線は凸でない辺を表わしている．普通の線では「山」折りに，破線では「谷」折りにする．このモデルでの辺の長さは，ある単位で 5, 10, 11, 12, 17 となっている．

曲面の剛性理論にはまだまだ驚きが残っている．ごく最近になって，コンリーとサビトフとウォルツは，曲面がこのようなジャバラ運動をするとき，曲面で囲まれる領域の**体積**が一定でなければならないことを，証明することに成功した．彼らの証明は代数的な機構を使った美しいものである（が，本書の扱う範囲にはない）．

参考文献

[1] A. コーシー：「多角形と多面体について，第 2 覚え書き」(*Sur les polygones et les polyèdres, seconde mémoire*), J. École Polytechnique XVIe Cahier, Tome IX (1813), 87; Œuvres Complètes, IIe Série, Vol. 1, Paris 1905, 26-38.

[2] R. コンリー：「多面体に対する剛性予想に対する反例」(*A counterexample to the rigidity conjecture for polyhedra*), Inst. Haut. Etud. Sci., Publ. Math. **47** (1978), 333-338.

[3] R. コンリー：「多面体の表面の剛性」(*The rigidity of polyhedral surfaces*), Mathematics Magazine **52** (1979), 275-283.

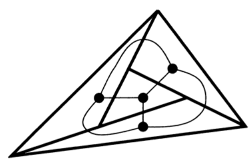
[4] R. コンリー，I. サビトフ，A. ウォルツ：「ジャバラ予想」(*The bellows conjecture*), Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry **38** (1997), 1-10.

[5] J. シェーンベルク，S. K. ザレンバ：「凸多角形に関するコーシーの補題について」(*On Cauchy's lemma concerning convex polygons*), Canadian J. Math. **19** (1967), 1062-1071.

第12章　触れ合う単体

$\mathbb{R}^d$ の中で，いくつの d 次元単体を互いに接触するように，つまり，それらの単体 2 つずつの共通部分がすべて $(d-1)$ 次元になるように，することができるか？

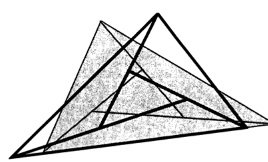
これは古くからある，非常に自然な問題である．この問題の解答である数を $f(d)$ と呼ぶ．まず，$f(1)=2$ は自明である．$d=2$ に対しては，余白の 4 つの三角形の配置によって，$f(2) \geq 4$ であることがわかる．5 つの三角形に対しては，同様の配置は存在しない．なぜなら，双対グラフを構成することにより，4 つの三角形の例から K_4 の平面グラフとしての図を描くことができるが，5 つの場合には K_5 の平面への埋め込みが得られることになる．しかしこれは不可能である（85 ページ参照）．こうして



$f(2) \geq 4.$

$$f(2)=4$$

となる．3 次元の場合，$f(3) \geq 8$ であることを見るのは大変易しい．そのためには，右に描いた 8 つの三角形の配置を使う．4 つの影のついた三角形と，「図が描かれている平面」の下方のある点 x とを結ぶと，平面に下から接触する 4 つの 4 面体が得られる．同様に 4 つの白い三角形も，図が描かれている平面の上方のある点 y と結ぶ．こうして，$\mathbb{R}^3$ の中に 8 つの触れ合う 4 面体が得られるので，$f(3) \geq 8$ となる．

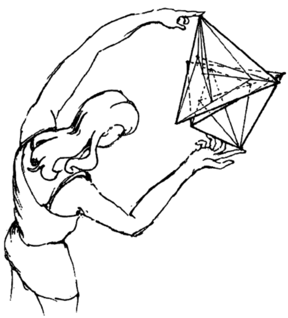


$f(3) \geq 8.$

1965 年に，バストンは $f(3) \leq 9$ を証明する本を書き，1991 年にはザクスが別の本を書いて，

$$f(3)=8$$

であることを確立した．$f(1) = 2$, $f(2) = 4$, $f(3) = 8$ とくれば，1956 年バジミールによって最初に提案された次の予想に到達するのに，たいしたインスピレーションは必要ではない．



「触れ合う単体」

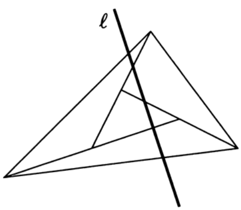
予想．$\mathbb{R}^d$ の中で配置し得る，どの 2 つも互いに接触する d 単体の最大個数は

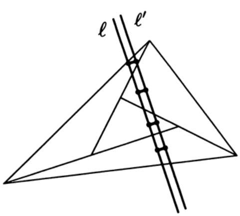
$$f(d) = 2^d$$

である．

下界 $f(d) \geq 2^d$ の証明は「ちゃんとやれば」難しくない．アフィンな座標変換をフルに使って，より強い次の（ザクス [4] による）結果を次元に関する帰納法で証明するのである．

定理 1．あらゆる $d \geq 2$ に対して，どの 2 つも互いに接触する 2^d 個の，$\mathbb{R}^d$ の d 単体の族であって，さらにどの単体の内部をも通過する横断的な直線を持つものが存在する．



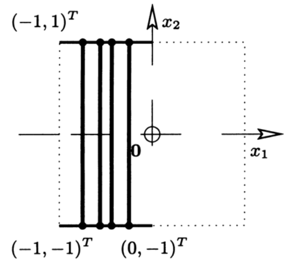


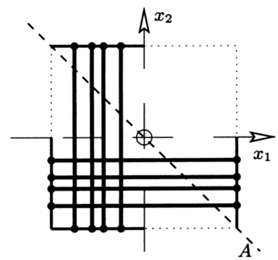
■ **証明．** $d = 2$ のとき，上で考えた 4 つの三角形の族にはそのような横断的な直線が存在している．今度は，横断的な直線 ℓ がある，d 次元の触れ合う単体の配置があったと考えよう．ℓ に十分近い平行線 ℓ' もまた横断的な直線である．ℓ' と ℓ を平行で，十分近くにとれば，各単体は，この 2 つの直線の間を垂直に結ぶ線分を含むことになる． 直線 ℓ, ℓ' のこの配置の単体に含まれる部分は有界なので，配置の外に 2 本の（ℓ, ℓ' を結ぶ）線分を追加して，この 2 本の外側にある線分で張られる長方形（つまりそれらの凸包）が他のすべての（ℓ, ℓ' を結ぶ）線分を含んでいるようにできる．こうして「梯子（はしご）」ができる．配置されている単体はそれぞれその内部に梯子のステップを 1 つ含んでおり，梯子の 4角（すみ）は配置の外側にあることになる．

さて，証明の主要な段階にきた．$\mathbb{R}^d$ を $\mathbb{R}^d$ に写す（アフィンな）座標変換を行い，梯子で張られる長方形を，

$$R^1 \ = \ \{(x_1, x_2, 0, \dots, 0)^T \ : \ -1 \leq x_1 \leq 0;\ -1 \leq x_2 \leq 1\}$$

で与えられる，下の図に示すような長方形（正方形の半分）に写す．こ





うすれば，$\mathbb{R}^d$ における触れ合う単体のこの配置 Σ^1 では，x_1 軸が横断的な直線になっており，各単体はその内部に線分

$$S^1(\alpha) \;=\; \{(\alpha, x_2, 0, \ldots, 0)^T : -1 \le x_2 \le 1\}$$

を含んでおり（$-1 < \alpha < 0$ を満たすある α に対して），原点 $\mathbf{0}$ はすべての単体の外側にある．

今度は，$x_1 = x_2$ によって与えられる超平面に関して，この配置の鏡映をとることで，もう 1 つの配置を作る．この第 2 の配置は x_2 軸を横断的な直線にしており，各単体はある $-1 < \beta < 0$ に対する線分

$$S^2(\beta) \;=\; \{(x_1, \beta, 0, \ldots, 0)^T : -1 \le x_1 \le 1\}$$

をその内部に含んでいる．しかし，各線分 $S^1(\alpha)$ は各線分 $S^2(\beta)$ と交わり，Σ^1 の各単体の内部の点は Σ^2 の各単体の内部と交わる．こうして，新しい $(d+1)$ 番目の座標 x_{d+1} を追加して，Σ を

$$\{\mathrm{conv}(P_i \cup \{-\boldsymbol{e}_{d+1}\}) : P_i \in \Sigma^1\} \;\cup\; \{\mathrm{conv}(P_j \cup \{\boldsymbol{e}_{d+1}\}) : P_j \in \Sigma^2\}$$

と置けば，$\mathbb{R}^{d+1}$ での触れ合う $(d+1)$ 単体の配置が得られる．さらに，反対対角線

$$A \;=\; \{(x, -x, 0, \ldots, 0)^T : x \in \mathbb{R}\} \;\subseteq\; \mathbb{R}^d$$

は，$S^1(\alpha)$ と $S^2(\beta)$ のすべての線分と交わっている．これを少し「傾け」て直線

$$L_\varepsilon \;=\; \{(x, -x, 0, \ldots, 0, \varepsilon x) : x \in \mathbb{R}\} \;\subseteq\; \mathbb{R}^{d+1}$$

を作れば，十分小さなすべての $\varepsilon > 0$ に対して，この直線は Σ のすべての単体に交わるようにできる．これで証明の帰納法の部分が終わった． □

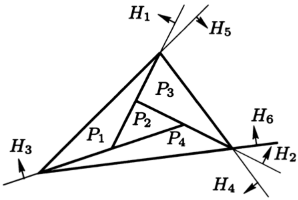
この指数関数的な下界とは対照的に，ゆるみのない上界を得ることは難しい．素朴な帰納法の議論（触れ合う単体の面となる超平面を別々に考えるというもの）では

$$f(d) \;\le\; \frac{2}{3}(d+1)!$$

が得られるだけで，これは定理 1 の下界からはかなり遠いものである．

しかし，ミーシャ・パールズはずっとよい上界に対する，以下の「魔法のような」証明を発見した．

定理 2. すべての $d \geq 1$ に対して $f(d) < 2^{d+1}$ となる．



■ **証明.** $\mathbb{R}^d$ の中に，r 個の触れ合う d 単体 $P_1, P_2, \ldots, P_r$ が配置されていたとする．まず，P_i の面によって張られる超平面を異なるものだけ $H_1, H_2, \ldots, H_s$ と数え上げ，それぞれに対して任意でよいから，正の側 H_i^+ を選び，もう一方の側を H_i^- と呼ぶことにする．

たとえば，余白に描いた $r = 4$ 個の三角形の 2 次元配置のときなら，$s = 6$ 枚の超平面（$d = 2$ だから直線だが）が得られる．

このデータから，次のように定義される（$\{+1, -1, 0\}$ に値をとる）成分を持つ $(r \times s)$ 行列である B **行列**を作る．

$$B_{ij} = \begin{cases} +1 & (P_i \text{ は} H_j \text{に含まれる面を持ち}, P_i \subseteq H_j^+), \\ -1 & (P_i \text{ は } H_j \text{に含まれる面を持ち}, P_i \subseteq H_j^-), \\ 0 & (P_i \text{ は } H_j \text{に含まれる面を持たない}). \end{cases}$$

たとえば，余白の 2 次元配置なら，行列

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ -1 & -1 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 \end{pmatrix}$$

が得られる．B 行列には，述べておくべき性質が 3 つある．第 1 に，あらゆる d 単体は $d+1$ 個の面を持つので，B の各行は常に，0 でない成分が $d+1$ 個と 0 の成分が $s-(d+1)$ 個ある．第 2 に，どの 2 つも触れ合っている単体を扱っているのだから，任意の行の対に対して，1 つの列があり，一方の行の成分は $+1$ で，もう一方の行の成分は -1 である．つまり，**0 である成分を無視したとしても**，行は互いに異なっている．第 3 に，B の第 i 行は単体 P_i を

$$P_i \;=\; \bigcap_{j: B_{ij}=1} H_j^+ \;\cap\; \bigcap_{j: B_{ij}=-1} H_j^- \qquad (*)$$

と「表わす」．

今度は，B から新しい行列 C を次のように作る．B の各行を，その

成分が 0 であるところを $+1$ か -1 に置き換えることで得られるすべてのベクトルで置き換える．B の各行の成分で 0 なのは $s-d-1$ 個なので，行列 C は $2^{s-d-1}r$ 行である．

上の例では，この行列 C は (32×6) 行列で，最初の部分は

$$C = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ \hline -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

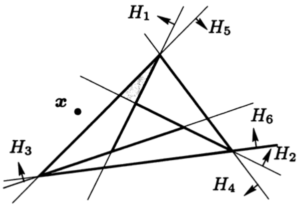
となっている．ここで，C の最初の 8 行は B の第 1 行から得られ，次の 8 行は B の第 2 行から得られ，などとなっている．

ここでポイントは，C のすべての行が異なっているということである．もし 2 つの行が同じ B の行から導かれたものなら，そこの 0 が異なる仕方で置き換えられているのだし，B の異なる行から導かれたものなら，0 をどのように置き換えたとしても異なっているわけである．しかし C の行は長さ s の，± 1 を成分とするベクトルであり，異なるとしても 2^s 個のベクトルしかあり得ない．こうして，C の行が互いに異なっているので，C は高々 2^s の行しか持てず，

$$2^{s-d-1}r \quad \leq \quad 2^s$$

となる．しかし，可能な ± 1 を成分とするベクトルがすべて C に現れるわけではなく，そのことから，等号のない不等式 $2^{s-d-1}r < 2^s$ が成り立ち，つまり，$r < 2^{d+1}$ が得られる．このことを見るために，C のあらゆる行が，B の行でと同様に，公式 $(*)$ によって，半空間の共通部分を表わしていることに注意する．この共通部分は，B の対応する行で与

えられる単体 P_i の部分集合である．どの超平面 H_j の上にもどの単体 P_i の中にもない点 $\boldsymbol{x} \in \mathbb{R}^d$ をとる．この $\boldsymbol{x}$ から，各 j に対し $\boldsymbol{x} \in H_j^+$ か $\boldsymbol{x} \in H_j^-$ に従って，+1 か −1 として，ベクトルを作ると，この ±1 を成分とするベクトルは C の行としては現れない．というのは，(*) 式で定まるその半空間の共通部分は $\boldsymbol{x}$ を含むから，どの単体 P_i にも含まれないことになる． □



行列 C の第 1 行は影のついた三角形を表わしているが，第 2 行は半空間の共通部分が空であることに対応している．点 $\boldsymbol{x}$ はベクトル

$$\begin{pmatrix} 1 & -1 & 1 & 1 & -1 & 1 \end{pmatrix}$$

に対応するが，これは行列 C には出てこない．

参考文献

[1] F. バジミール：「隣り合う 4 面体に関する予想」(*A conjecture concerning neighboring tetrahedra*), Amer. Math. Monthly **63** (1956) 328-329.

[2] V. J. D. バストン：『ユークリッド空間における多面体のいくつかの性質』(*Some Properties of Polyhedra in Euclidean Space*), Pergamon Press, Oxford 1965.

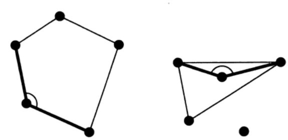
[3] M. A. パールズ：「E^d における高々2^{d+1} 個の隣り合う単体」(*At most 2^{d+1} neighborly simplices in E^d*), Annals of Discrete Math. **20** (1984), 253-254.

[4] J. ザクス：「E^d における 2^d 個の d 単体の隣り合う族」(*Neighborly families of 2^d d-simplices in E^d*), Geometriae Dedicata **11** (1981), 279-296.

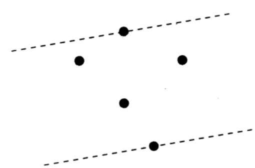
[5] J. ザクス：「9 つの隣り合う 4 面体は存在しない」(*No nine neighborly tetrahedra exist*), Memoirs Amer. Math. Soc. No. 447, Vol. 91, 1991.

第13章　大きな点集合は鈍角を持つ

1950年頃，ポール・エルデシュは，$\mathbb{R}^d$ における 2^d 個より多くの点の集合があれば，少なくとも1つの**鈍角**，つまり，$\frac{\pi}{2}$ よりも大きい角が定まる，という予想をした．言い換えれば，(直角も含む) 鋭角しか持たない $\mathbb{R}^d$ の点の集合の大きさは高々 2^d であるというものである．この問題はオランダ数学会の「懸賞問題」として出されたものだが，受け取った解答は $d = 2$ と $d = 3$ に対するものだけであった．



$d = 2$ のときには問題は易しい．5点が凸の5角形を定めるかも知れないが，それはいつでも1つの鈍角を持っている（実際，1つの角は少なくとも 108° である）．そうでなければ，三角形をなす3点の凸包に含まれてしまう点が1つある．しかし，この点は三角形の3つの角を見込むが，その間の角の和は 360° になり，少なくとも 120° 以上の角が1つはある．(このあとの場合には3点が直線上にある場合も含まれていて，そのときには 180° の角がある.)



これとは無関係に，数年後ヴィクトール・クリーは1つの質問をし，ポール・エルデシュがそれを拡張して，次の意味での「対蹠性」を持つ $\mathbb{R}^d$ の点集合がどれほど大きくなり得るか，という問題にした.「点集合の**任意の**2点に対して，その集合を含む（2つの平行な超平面を境界とする）帯で，その2点が別の側の境界上にあるものがある」という性質を考えるのである．

その後，1962年に，ルードヴィッヒ・ダンツァーとブランコ・グリュンバウムは両方の問題を一撃で解決してしまった．彼らは両方の最大サイズを不等式の連鎖の中に挟み込み，連鎖の始めと終わりを 2^d にしたのである．つまり，エルデシュの問題に対してもクリーの問題に対して

も答えは 2^d である．

以下で，(有限の) 点集合 $S \subseteq \mathbb{R}^d$ とその凸包 $\mathrm{conv}(S)$，そして一般の凸の多面体 $Q \subseteq \mathbb{R}^d$ を考える．(基本的な概念については，64 ページの多面体に関する箱を参照のこと．) これらの集合が全体の次元 d を持つ，つまり，ある超平面に含まれることはないと仮定する．そのような集合が**触れ合う**とは，少なくとも 1 点は共通の境界点を持つが，内部同士は交わらないときとする．任意の集合 $Q \subseteq \mathbb{R}^d$ とベクトル $\boldsymbol{s} \in \mathbb{R}^d$ に対して，$\mathbf{0}$ を $\boldsymbol{s}$ に移す平行移動による Q の像を $Q + \boldsymbol{s}$ と表わす．同じように，$Q - \boldsymbol{s}$ は $\boldsymbol{s}$ を原点に移す平行移動で写されたものである．

あまり脅(おび)えないで欲しい．この章は，d 次元の幾何への散策だが，以下の議論にはどんな意味でも「高次元の直観」の必要はない．というのは，その議論にはすべてついていくことができるし，3 次元で，いや 2 次元でも視覚化され (て，**理解**もされ) る．それゆえ，我々の図は $d = 2$ (このとき「超平面」は直線) に対する証明の説明になっているし，$d = 3$ (このとき「超平面」は平面) に対する絵も描くことができるだろう．

定理 1．あらゆる d に対して，次の不等式の連鎖が得られる．

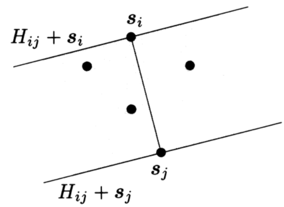
$$
\begin{aligned}
2^d &\overset{(1)}{\leq} \max \# \left\{ S \subseteq \mathbb{R}^d \;\middle|\; \begin{array}{l} \text{任意の } \{\boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{s}_k\} \subseteq S \text{ に対して} \\ \sphericalangle(\boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{s}_k) \leq \frac{\pi}{2}. \end{array} \right\} \\
&\overset{(2)}{\leq} \max \# \left\{ S \subseteq \mathbb{R}^d \;\middle|\; \begin{array}{l} \text{任意の 2 点 } \{\boldsymbol{s}_i, \boldsymbol{s}_j\} \subseteq S \text{ に対して，} S \text{ を含} \\ \text{む帯 } \mathcal{S}(i,j) \text{ で，} \boldsymbol{s}_i \text{ と } \boldsymbol{s}_j \text{ が } \mathcal{S}(i,j) \text{ の平行} \\ \text{な境界超平面上にあるものが存在する．} \end{array} \right\} \\
&\overset{(3)}{=} \max \# \left\{ S \subseteq \mathbb{R}^d \;\middle|\; \begin{array}{l} P = \mathrm{conv}(S) \text{ の平行移動像 } P - \boldsymbol{s}_i \text{ は互い} \\ \text{に 1 点で交わるが，触れ合うのみ．} \end{array} \right\} \\
&\overset{(4)}{\leq} \max \# \left\{ S \subseteq \mathbb{R}^d \;\middle|\; \begin{array}{l} \text{ある } d \text{ 次元の凸多面体 } Q \subseteq \mathbb{R}^d \text{ の平行移動} \\ \text{像 } Q + \boldsymbol{s}_i \text{ は，どの 2 つも互いに触れ合う} \\ \text{のみ．} \end{array} \right\} \\
&\overset{(5)}{=} \max \# \left\{ S \subseteq \mathbb{R}^d \;\middle|\; \begin{array}{l} \text{ある } d \text{ 次元の点対称な凸多面体 } Q^* \subseteq \mathbb{R}^d \text{ の} \\ \text{平行移動像 } Q^* + \boldsymbol{s}_i \text{ は，どの 2 つも互いに} \\ \text{触れ合うのみ．} \end{array} \right\} \\
&\overset{(6)}{\leq} 2^d.
\end{aligned}
$$

■ **証明.** 証明すべきは 6 つの主張（等式と不等式）である．では，始めよう．

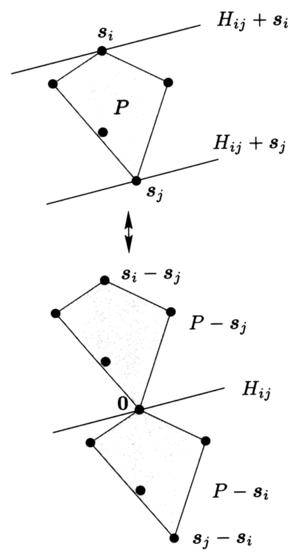
(1) $S=\{0,1\}^d$ を $\mathbb{R}^d$ の標準的な単位立方体の頂点集合とし，$\boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{s}_k \in S$ を選ぶ．対称性により，$\boldsymbol{s}_j=\mathbf{0}$ が零ベクトルであると仮定してよい．それゆえ，角は

$$\cos\sphericalangle(\boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{s}_k)=\frac{\langle \boldsymbol{s}_i, \boldsymbol{s}_k\rangle}{|\boldsymbol{s}_i||\boldsymbol{s}_k|}$$

と計算できるが，これは明らかに非負である．こうして，集合 S は $|S|=2^d$ を満たし，鈍角は持っていない．



(2) S が鈍角を含まないなら，どんな $\boldsymbol{s}_i, \boldsymbol{s}_j \in S$ に対しても，$H_{ij}+\boldsymbol{s}_i$ と $H_{ij}+\boldsymbol{s}_j$ を，それぞれ $\boldsymbol{s}_i$ と $\boldsymbol{s}_j$ を通る平行な超平面で，辺 $[\boldsymbol{s}_i, \boldsymbol{s}_j]$ に垂直なものとして定義してもよい．ここで，$H_{ij}=\{\boldsymbol{x}\in\mathbb{R}^d : \langle \boldsymbol{x}, \boldsymbol{s}_i-\boldsymbol{s}_j\rangle=0\}$ は**原点を通り**，$\boldsymbol{s}_i$ と $\boldsymbol{s}_j$ を通る直線に垂直な超平面であり，$H+\boldsymbol{s}_j=\{\boldsymbol{x}+\boldsymbol{s}_j : \boldsymbol{x}\in H\}$ は H の平行移動像で点 $\boldsymbol{s}_j$ を通るものである．それゆえ，$H_{ij}+\boldsymbol{s}_i$ と $H_{ij}+\boldsymbol{s}_j$ の間の帯はまさに，$\boldsymbol{s}_i$ と $\boldsymbol{s}_j$ を除いて，角 $\sphericalangle(\boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{x})$ と $\sphericalangle(\boldsymbol{s}_j, \boldsymbol{s}_i, \boldsymbol{x})$ が鈍角でないようなすべての点 $\boldsymbol{x}\in\mathbb{R}$ からなっている．こうして，この帯は S 全体を含んでいる．



(3) P が $\boldsymbol{s}_i$ を含む $H_{ij}+\boldsymbol{s}_j$ の（定める）半空間に含まれるのは，$P-\boldsymbol{s}_j$ が $\boldsymbol{s}_i-\boldsymbol{s}_j$ を含む H_{ij} の半空間に含まれるとき，かつそのときに限る．「ある物体がある半空間に含まれる」という性質は，物体と半空間を同じだけ（今は $-\boldsymbol{s}_j$ だけ）平行移動させても壊れないからである．同様に，P が $\boldsymbol{s}_j$ を含む $H_{ij}+\boldsymbol{s}_i$ の半空間に含まれるのは，$P-\boldsymbol{s}_i$ が $\boldsymbol{s}_j-\boldsymbol{s}_i$ を含む H_{ij} の半空間に含まれるとき，かつそのときに限る．

2 つの主張を合わせると，多面体 P が $H_{ij}+\boldsymbol{s}_i$ と $H_{ij}+\boldsymbol{s}_j$ の間の帯に含まれるのは，$P-\boldsymbol{s}_i$ と $P-\boldsymbol{s}_j$ が超平面 H_{ij} に関して異なる半空間に属すとき，かつそのときに限ることがわかる．

余白のスケッチはこの対応の説明である．

さらに，$\boldsymbol{s}_i\in P=\mathrm{conv}(S)$ であることから，原点 $\mathbf{0}$ はすべての平行移動像 $P-\boldsymbol{s}_i$ $(\boldsymbol{s}_i\in S)$ に含まれることになる．こうして，集合 $P-\boldsymbol{s}_i$ は $\mathbf{0}$ で交わるが，触れ合うのみである．つまり，2 つずつ考えると，内部は交わらない．なぜなら，それらは対応する超平面 H_{ij} の反対の側にあることになるからである．

(4) ここは何もしなくてもよい．「平行移動像が 2 つずつ触れ合うべし」

という条件は,「それらが共通の点で交わるが触れ合うのみ」というより弱いからである．同じように，P を $\mathbb{R}^d$ の任意の凸d多面体とすれば，条件は弱くなる．さらに，S は $-S$ に取り換えてもよい．

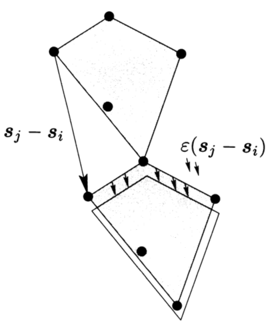
(5) ここで,「$\geq$」であることは自明だが，それは我々にとって興味ある方向ではない．配置 $S \subseteq \mathbb{R}^d$ と任意の d 多面体 $Q \subseteq \mathbb{R}^d$ で，平行移動像 $Q + \boldsymbol{s}_i$ $(\boldsymbol{s}_i \in S)$ が 2 つずつ触れ合っているものから始めるべきである．この状況では，Q の代わりに

$$Q^* = \left\{\tfrac{1}{2}(\boldsymbol{x} - \boldsymbol{y}) \in \mathbb{R}^d : \boldsymbol{x}, \boldsymbol{y} \in Q\right\}$$

を使うことができるというのが主張である．しかし，これを見るのは難しくない．まず，Q^* は d 次元の，凸で点対称な多面体である．Q^* が多面体である（その頂点は，Q の頂点 $\boldsymbol{q}_i, \boldsymbol{q}_j$ に対する，$\frac{1}{2}(\boldsymbol{q}_i - \boldsymbol{q}_j)$ の形のもの）ことを確かめることはできるが，このことは重要ではない．

今度は，$Q + \boldsymbol{s}_i$ と $Q + \boldsymbol{s}_j$ が触れ合うのが，$Q^* + \boldsymbol{s}_i$ と $Q^* + \boldsymbol{s}_j$ が触れ合う**とき，かつそのときに限る**ことを示す．このために，ミンコフスキーにならって，以下のことに注意する．

$$\begin{aligned}
&(Q^* + \boldsymbol{s}_i) \cap (Q^* + \boldsymbol{s}_j) \neq \emptyset \\
&\qquad \Longleftrightarrow \; \exists\, \boldsymbol{q}_i', \boldsymbol{q}_i'', \boldsymbol{q}_j', \boldsymbol{q}_j'' \in Q : \tfrac{1}{2}(\boldsymbol{q}_i' - \boldsymbol{q}_i'') + \boldsymbol{s}_i = \tfrac{1}{2}(\boldsymbol{q}_j' - \boldsymbol{q}_j'') + \boldsymbol{s}_j \\
&\qquad \Longleftrightarrow \; \exists\, \boldsymbol{q}_i', \boldsymbol{q}_i'', \boldsymbol{q}_j', \boldsymbol{q}_j'' \in Q : \tfrac{1}{2}(\boldsymbol{q}_i' + \boldsymbol{q}_j'') + \boldsymbol{s}_i = \tfrac{1}{2}(\boldsymbol{q}_j' + \boldsymbol{q}_i'') + \boldsymbol{s}_j \\
&\qquad \Longleftrightarrow \; \exists\, \boldsymbol{q}_i, \boldsymbol{q}_j \in Q : \boldsymbol{q}_i + \boldsymbol{s}_i = \boldsymbol{q}_j + \boldsymbol{s}_j \\
&\qquad \Longleftrightarrow \; (Q + \boldsymbol{s}_i) \cap (Q + \boldsymbol{s}_j) \neq \emptyset
\end{aligned}$$



ここで，第 3 の（そして決定的な）同値性「$\Longleftrightarrow$」では,「$\Leftarrow$」を得るのに，あらゆる $\boldsymbol{q} \in Q$ が $\boldsymbol{q} = \frac{1}{2}(\boldsymbol{q} + \boldsymbol{q})$ と書くことができることを,「$\Rightarrow$」を見るのに，Q が凸なので，$\frac{1}{2}(\boldsymbol{q}_i' + \boldsymbol{q}_j''), \frac{1}{2}(\boldsymbol{q}_j' + \boldsymbol{q}_i'') \in Q$ であることを使っている．

こうして，Q から Q^* に移行すること（**ミンコフスキーの対称化**として知られる）で，2 つの平行移動像 $Q + \boldsymbol{s}_i$ と $Q + \boldsymbol{s}_j$ が交わるという性質が保たれている．つまり，任意の凸集合 Q に対して，2 つの平行移動像 $Q + \boldsymbol{s}_i$ と $Q + \boldsymbol{s}_j$ が交わるのは，平行移動像 $Q^* + \boldsymbol{s}_i$ と $Q^* + \boldsymbol{s}_j$ が交わるとき，かつそのときに限る，ということを示したのである．

次の特徴付けはまた，ミンコフスキーの対称化が，2 つの平行移動像が触れ合うという性質も保つことを示している．

> **$Q+s_i$ と $Q+s_j$ が触れ合うことは，それらは交わるが，任意の $\varepsilon>0$ に対して $Q+s_i$ と $Q+s_j+\varepsilon(s_j-s_i)$ は交わらないとき，かつそのときに限る．**

(6) Q^*+s_i と Q^*+s_j が触れ合うと仮定する．あらゆる交点

$$x \in (Q^*+s_i)\cap(Q^*+s_j)$$

に対して，

$$x-s_i \in Q^* \quad \text{かつ} \quad x-s_j \in Q^*$$

となり，Q^* は点対称だから，

$$s_i - x = -(x-s_i) \in Q^*$$

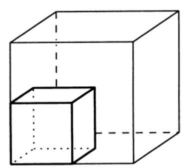
となり，それゆえ，Q^* は凸だから，

$$\tfrac{1}{2}(s_i-s_j) = \tfrac{1}{2}\left((x-s_j)+(s_i-x)\right) \in Q^*$$

となる．すべての i に対して，$\frac{1}{2}(s_i+s_j)$ が Q^*+s_j に含まれるという結論が得られる．結局，$P=\mathrm{conv}(S)$ に対して

$$P_j = \tfrac{1}{2}(P+s_j) = \mathrm{conv}\left\{\tfrac{1}{2}(s_i+s_j) : s_i \in S\right\} \subseteq Q^*+s_j$$

となり，このことは集合 $P_j=\frac{1}{2}(P+s_j)$ が触れ合えるだけであることを意味している．



縮尺 $\frac{1}{2}$，$\mathrm{vol}(P_j)=\frac{1}{8}\mathrm{vol}(P)$.

最後に，集合 P_j はすべて P に含まれる．なぜなら，P が凸なので，点 s_i, s_j, $\frac{1}{2}(s_i+s_j)$ が P に属すからである．しかし，P_j は P を平行移動して相似縮小したもので，P に含まれている．相似比は $\frac{1}{2}$ であり，d 次元の集合を扱っているのだから，

$$\mathrm{vol}(P_j) \quad = \quad \frac{1}{2^d}\mathrm{vol}(P)$$

となる．つまり，P には高々 2^d 個の集合 P_j しか詰められないということであり，それゆえ $|S| \le 2^d$ である．

不等式の連鎖が閉じ，証明が完成する． □

... しかし，話はこれで終わりではない．ダンツァーとグリュンバウムは次の自然な疑問を問題にした．

もし，すべての角を単に鈍角でないとするのでなく鋭角と，つまり，直角を禁止したとすれば，どうなるのだろうか？

彼らは，鋭角しか持たない $\mathbb{R}^d$ の中の $2d-1$ 個の点の配置を構成し，これが最善の値であろうという予想をした．グリュンバウムは，$d \leq 3$ のときは実際これが正しいことを証明した．しかし，21 年後の 1983 年に，ポール・エルデシュとツォルタン・フュレディは，次元が高ければ（！）この予想が間違っていることを，きわめて劇的に示したのである．彼らの方法は，確率論的な議論の強力さの偉大な例になっている．「確率論的方法」について知りたい読者は，第 32 章を参照のこと．

定理 2. **あらゆる** $d \geq 1$ **に対して，鋭角しか定めない，**$\mathbb{R}^d$ **の** $\lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^d \rfloor$ **個の（単位** d **立方体の頂点である）点の集合** $S \subseteq \{0,1\}^d$ **が存在する．**

とくに $d = 35$ **次元のとき，鋭角だけしか持たない** $76 > 2{\cdot}35 - 1$ **個の点の集合が存在する．**

■ **証明.** $m = \lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^d \rfloor$ とおき，$2m$ 個のベクトル

$$\boldsymbol{x}(1), \boldsymbol{x}(2), \ldots, \boldsymbol{x}(2m) \;\in\; \{0,1\}^d$$

をとる．その際，その座標のすべてを，独立かつランダムに，0 か 1 になるように，それぞれ確率 $\frac{1}{2}$ で選ぶことにする．(このために，完全なコインを $2md$ 回投げてもよい．d が大きいと，多分すぐに嫌になるだろうが.)

さて，3 つのベクトル $\boldsymbol{x}(i), \boldsymbol{x}(j), \boldsymbol{x}(k)$ が $\boldsymbol{x}(j)$ を頂点として直角を作るのは，スカラー積

$$\left\langle\, \boldsymbol{x}(i) - \boldsymbol{x}(j),\; \boldsymbol{x}(k) - \boldsymbol{x}(j) \,\right\rangle$$

が 0 となるとき，かつそのときに限る，つまり，各座標 ℓ に対して

$$x(i)_\ell - x(j)_\ell = 0 \quad \text{または} \quad x(k)_\ell - x(j)_\ell = 0$$

であるなら，直角になる．この等式を満たすとき，(i,j,k) を**悪い 3 つ組**と呼ぶ．($\boldsymbol{x}(i) = \boldsymbol{x}(j)$ または $\boldsymbol{x}(j) = \boldsymbol{x}(k)$ であれば，角は定義できないが，そのときも 3 つ組は確かに悪いわけである.)

ある特定の3つ組が悪い3つ組である確率は $\left(\frac{3}{4}\right)^d$ である．実際，それがよい3つ組であるのは，$2d$ 個の座標のうちの1つの ℓ に対して，

$$x(i)_\ell = x(k)_\ell = 0, \quad x(j)_\ell = 1$$
$$\text{かまたは} \quad x(i)_\ell = x(k)_\ell = 1, \quad x(j)_\ell = 0$$

が成り立つとき，かつそのときに限る．このことから，同じ程度に確からしい8つの選択の中から悪い選択は6つとなり，ある3つ組が悪いのは，（確率 $\frac{3}{4}$ で起こる）悪い選択が d 個の座標それぞれに対して起こるとき，かつそのときに限ることになる．

考えなければならない3つ組の数は $3\binom{2m}{3}$ である．というのは，3つのベクトルの集合は $\binom{2m}{3}$ 個あり，それぞれに頂点をどれにするかの3つの選択肢があるからである．もちろん，色々な3つ組が悪い3つ組になる確率は独立ではないが，**期待値の線形性**（期待値とは，可能なすべての選択に関する平均をとることで，附録を参照のこと）によって，悪い3つ組の**期待値**は $3\binom{2m}{3}\left(\frac{3}{4}\right)^d$ となる．つまり（ここが確率論的方法が力を発揮する場所），高々 $3\binom{2m}{3}\left(\frac{3}{4}\right)^d$ 個の悪い3つ組を持つ，**ある** $2m$ 個のベクトルの選び方が存在する．ここで，m の選び方から

$$3\binom{2m}{3}\left(\frac{3}{4}\right)^d \; < \; 3\frac{(2m)^3}{6}\left(\frac{3}{4}\right)^d \; = \; m(2m)^2\left(\frac{3}{4}\right)^d \; \leq \; m$$

となる．

しかし，悪い3つ組が m 個以下なら，$2m$ 個のベクトル $\boldsymbol{x}(i)$ から m 個を取り除いて，残りの m 個のベクトルには悪い3つ組を含まないように，つまり，鋭角しか定めないようにすることができる． □

附録：確率論から3つのツール

ここで，離散的確率論から3つの基本的なツール，確率変数，期待値の線形性，マルコフの不等式，をまとめておこう．これらのツールはこれから，何度も出てくることになる．

(Ω, p) を有限の**確率空間**とする．つまり，Ω は有限集合で，$p = \mathrm{Prob}$ は Ω から区間 $[0,1]$ への写像で，$\sum_{\omega\in\Omega} p(\omega) = 1$ を満たすとする．Ω 上の**確率変数** X とは写像 $X : \Omega \longrightarrow \mathbb{R}$ のことである．像の集合 $X(\Omega)$ の上に，$p(X = x) = \sum_{X(\omega)=x} p(\omega)$ と置くことによって，確率空間を

定義する．簡単な例としては，偏りのないサイコロ（すべて $p(\omega)=\frac{1}{6}$）で，$X=$「投げたサイコロの上面の数」としたものがある．

X の**期待値** EX とは平均として期待されるものであり，つまり，

$$EX = \sum_{\omega\in\Omega} p(\omega)X(\omega)$$

のことである．さて，X と Y を Ω 上の2つの確率変数とすると，その和 $X+Y$ も確率変数であり，

$$\begin{aligned} E(X+Y) &= \sum_{\omega} p(\omega)(X(\omega)+Y(\omega)) \\ &= \sum_{\omega} p(\omega)X(\omega) + \sum_{\omega} p(\omega)Y(\omega) = EX + EY \end{aligned}$$

が得られる．明らかに，このことは確率変数の任意有限個の1次結合に拡張することができる．これが**期待値の線形性**と呼ばれるものである．確率変数がどのような意味でも「独立」でなければならないという仮定が必要ないことに注意する！

第3のツールは，非負の値しかとらないような確率変数 X（このとき短く $X\geq 0$ と書く）に関するものである．

$$\mathrm{Prob}(X\geq a) = \sum_{\omega:X(\omega)\geq a} p(\omega)$$

を，X が少なくともある $a>0$ だけの大きさである確率とする．そのとき，

$$EX = \sum_{\omega:X(\omega)\geq a} p(\omega)X(\omega) + \sum_{\omega:X(\omega)<a} p(\omega)X(\omega) \geq a\sum_{\omega:X(\omega)\geq a} p(\omega)$$

となって，証明された

$$\mathrm{Prob}(X\geq a) \leq \frac{EX}{a}$$

は**マルコフの不等式**と呼ばれる．

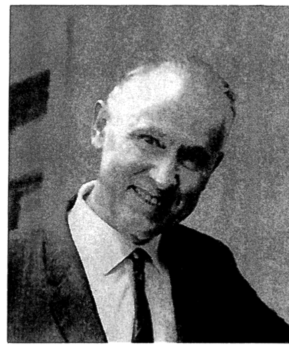
参考文献

[1] L. ダンツァー, B. グリュンバウム:「P. エルデシュと V. L. クリーの凸体に関する 2 つの問題について」(*Über zwei Probleme bezüglich konvexer Körper von P. Erdös und von V. L. Klee*), Math. Zeitschrift **79** (1962), 95-99.

[2] P. エルデシュ, Z. フュレディ:「d 次元ユークリッド空間における n 点の間の最大角」(*The greatest angle among n points in the d-dimensional Euclidean space*), Annals of Discrete Mathematics **17** (1983), 275-283.

[3] H. ミンコフスキー:「合同な立体の最密の格子状配置」(*Dichteste gitterförmige Lagerung kongruenter Körper*), Nachrichten Ges. Wiss. Göttingen, Math.-Phys. Klasse 1904, 311-355.

第14章　ボルスク予想



カロル・ボルスク

1933年のカロル・ボルスクの論文「n次元ユークリッド球面についての3つの定理」は，(スタニスウォフ・ウラムによって予想され）今日ボルスク–ウラムの定理として知られている重要な結果

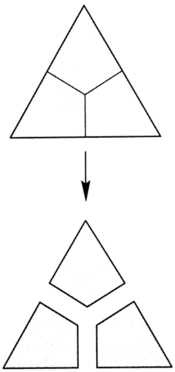
> **あらゆる連続写像 $f: S^d \to \mathbb{R}^d$ は球面 S^d のある2つの対蹠点を $\mathbb{R}^d$ の同じ点に写す**

を含んでいることで有名である．この論文はまた，その最後に，ボルスク予想として知られるようになった次の問題が提案されていることによっても有名である．

> **有限の直径 $\mathrm{diam}(S) > 0$ を持つあらゆる集合 $S \subseteq \mathbb{R}^d$ を，より小さな直径を持つ高々 $d+1$ 個の集合に分割することができるか？**

この $d+1$ という限界は最良である．もし S が正則な d 次元単体，もしくはその $d+1$ 個の頂点からなる集合であれば，直径が小さな分割では，どの部分も単体の頂点を2つ以上含むことはできないからである．$f(d)$ で，あらゆる有界な集合 $S \subseteq \mathbb{R}^d$ が直径のより小さな $f(d)$ 個の部分への分割を持つ中での最小数を表わすとすると，正則な単体の例から $f(d) \geq d+1$ であることがわかる．

ボルスク予想は，S が球面の場合（ボルスク自身によって），滑らかな物体 S の場合（ボルスク–ウラムの定理を使って），$d \leq 3$ の場合は ... と証明されてきたが，一般的な予想は未解決のままである．$f(d)$ に対する有効な最善の上界が，オーデッド・シュラムによって与えられた．



どんな d 単体も，直径がより小さい $d+1$ 個の部分に分割することが可能である．



A. ニリー

十分大きなすべての d に対して，

$$f(d) \leq (1.23)^d$$

となるというものである．この上界は予想「$f(d) = d+1$」に比べてとても弱そうに見えるが，1993 年にジェフ・カーンとギル・カライによってボルスク予想が誤りであると証明されて，突然もっともらしく見えてきた．ボルスクの論文から 60 年経って，カーンとカライは，十分大きな d に対して $f(d) \geq (1.2)^{\sqrt{d}}$ であることを証明した．

天書版のカーン–カライの証明が，A. ニリーによって与えられた．短い上に，他を参照する必要のない証明で，$d = 946$ 次元の次元におけるボルスク予想の具体的な反例も与えている．ここでは，この証明を改良したものを示すことにする．この改良は，アンドレイ・M・ライゴロツキーとベルヌルフ・ヴァイスバッハによるもので，次元を $d = 561$，さらには $d = 560$ にまで下げている．$d = 323$ という新しい「記録」が，2000 年の夏にアイク・ヒンリクスによって得られている．

定理． $q = p^m$ **を素数ベキとし，** $n = 4q-2$, $d = \binom{n}{2} = (2q-1)(4q-3)$ **とおく．そのとき，**$\mathbb{R}^d$ **の** 2^{n-2} **個の点の作る集合** $S \subseteq \{+1,-1\}^d$ **で，**S **より小さな直径を持つ部分へ** S **を分割すると，少なくとも，**

$$\frac{2^{n-2}}{\sum_{i=0}^{q-2} \binom{n-1}{i}}$$

個の部分に分かれるものが存在する．$q = 9$ **のとき，このことは** $d = 561$ **でボルスク予想が誤りであることを示している．さらに，十分大きなすべての** d **に対し，**$f(d) > (1.2)^{\sqrt{d}}$ **が成り立つ．**

■ **証明．** 集合 S の構成は 4 段階で行う．

(1) q を素数ベキで，$n = 4q-2$ とし，

$$Q \;=\; \Big\{\boldsymbol{x} \in \{+1,-1\}^n : x_1 = 1,\ \#\{i : x_i = -1\} \text{ は偶数}\Big\}$$

とおく．

この Q は $\mathbb{R}^n$ の 2^{n-2} 個のベクトルの作る集合である．すべてのベクトル $\boldsymbol{x}, \boldsymbol{y} \in Q$ に対して，$\langle \boldsymbol{x}, \boldsymbol{y} \rangle \equiv 2 \pmod 4$ が成り立つことを示す．$|\langle \boldsymbol{x}, \boldsymbol{y} \rangle| = 2$ を満たす $\boldsymbol{x}, \boldsymbol{y}$ を**ほとんど直交**していると言う．ほ

とんど直交しているベクトルを含まないような部分集合 $Q' \subseteq Q$ は $|Q'| \le \sum_{i=0}^{q-2} \binom{n-1}{i}$ を満たすほど「小さく」なければならないことを証明する．

ベクトル，行列，スカラー積

ここでは，すべてのベクトル $\boldsymbol{x}, \boldsymbol{y}, \ldots$ は列ベクトルを表わしている．転置ベクトル $\boldsymbol{x}^T, \boldsymbol{y}^T, \ldots$ は行ベクトルである．行列の積 $\boldsymbol{x}\boldsymbol{x}^T$ はランク 1 の行列で，$(\boldsymbol{x}\boldsymbol{x}^T)_{ij} = x_i x_j$ となる[1]．$\boldsymbol{x}, \boldsymbol{y}$ が列ベクトルなら，そのスカラー積は

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle \;=\; \sum_i x_i y_i \;=\; \boldsymbol{x}^T \boldsymbol{y}$$

である．また行列 $X, Y \in \mathbb{R}^{n\times n}$ に対するスカラー積も必要となる．それは行列を長さ n^2 のベクトルと解釈して，そのスカラー積

$$\langle X, Y \rangle \;=\; \sum_{i,j} x_{ij} y_{ij}$$

をとる．

$$\boldsymbol{x} = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \implies$$

$$\boldsymbol{x}^T = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 \end{pmatrix}$$

$$\boldsymbol{x}\boldsymbol{x}^T = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \end{pmatrix}$$

(2) Q から，2^{n-2} 個のランク 1 の対称 $(n \times n)$ 行列の集合

$$R \;=\; \{\boldsymbol{x}\boldsymbol{x}^T : \boldsymbol{x} \in Q\}$$

を作る．これを，n^2 個の成分を持つベクトルとみて，$R \subseteq \mathbb{R}^{n^2}$ と考える．これらのベクトルの間の角が常に鋭角であることを示す．その際，ベクトルのスカラー積が正で，4 以上であることを示すことにする．さらに，$R' \subseteq R$ が，最小のスカラー積である 4 を与えるような 2 つのベクトルを含まないならば，$|R'|$ は「小さく」，$|R'| \le \sum_{i=0}^{q-2} \binom{n-1}{i}$ を満たす．

(3) R から，対応する行列の対角線より下にある成分を座標とする $\mathbb{R}^{\binom{n}{2}}$ の点全体の集合 S が得られる．つまり，

---

[1] ［訳註］もちろん，$\boldsymbol{x} \in \mathbb{R}^n$ なら，$\boldsymbol{x}\boldsymbol{x}^T$ は $n \times n$ 行列である．

$$S \;=\; \{(\boldsymbol{x}\boldsymbol{x}^T)_{i>j} : \boldsymbol{x}\boldsymbol{x}^T \in R\}$$

を考える．S はまた 2^{n-2} 個の点からなる．これらの点の間の最大の距離はまさに，ほとんど直交するベクトル $\boldsymbol{x}, \boldsymbol{y} \in Q$ に対するものになる．より小さな直径を持つ部分集合 $S' \subseteq S$ は「小さく」，$|S'| \le \sum_{i=0}^{q-2} \binom{n-1}{i}$ を満たさねばならないという結論が得られる．

(4) 評価． (3) から，S をより小さな直径の部分集合へ分割するには少なくとも

$$g(q) \;=\; \frac{2^{4q-4}}{\sum_{i=0}^{q-2} \binom{4q-3}{i}}$$

個の部分が必要であることがわかる．こうして，

$$f(d) \;\ge\; \max\{g(q), d+1\} \qquad (d \;=\; (2q-1)(4q-3) \text{ に対して})$$

となる．したがって，$g(q) \;>\; (2q-1)(4q-3)+1$ であれば，$d = (2q-1)(4q-3)$ 次元におけるボルスク予想の反例が得られることになる．

あとの計算で $g(9) > 562$ を示すが，このことから $d = 561$ 次元に反例があることがわかる．また，

$$g(q) \;>\; \frac{e}{64\,q^2}\left(\frac{27}{16}\right)^q$$

を計算で示すが，これから十分大きな d に対する漸近的な限界 $f(d) > (1.2)^{\sqrt{d}}$ が得られる．

(1) の詳しい証明． 可除性に関する無害な，いくつかの考察から始めよう．

補題． **関数 $P(z) = \binom{z-2}{q-2}$ は $q-2$ 次の多項式であり，すべての整数 z に対して整数値をとる．整数 $P(z)$ が p で割り切れるのは，z が q を法として 0 か 1 に合同でないとき，かつそのときに限る．**

■ **証明．** このために 2 項係数を

$$P(z) \;=\; \binom{z-2}{q-2} \;=\; \frac{(z-2)(z-3)\cdot\cdots\cdot(z-q+1)}{(q-2)(q-3)\cdot\quad\cdots\quad\cdots\quad\cdot 2\cdot 1} \qquad (*)$$

と書き，分母と分子の p 因数の数を比較する．分母は $(q-2)!$ と同じ数の p 因数を持っており，それはまた $(q-1)!$ とも同じ数である．というのは，$q-1$ は p では割れないからである．実際，余白の主張により，q を法とする 0 でない各剰余類から 1 つずつとったどんな $q-1$ 個の整数の積をとっても，p 因数の数は同じになる．

主張． $a \equiv b \not\equiv 0 \pmod{q}$ ならば，a と b の素因数分解で p のベキは同じ数だけある．

■ **証明．** $a = b + sp^m$ となっている．ここで，b は $p^m = q$ では割り切れない．すると，b の約数であるベキ p^k は $k < m$ を満たし，a の約数でもある．主張は a と b について対称である．□

さて，z が 0 か 1 と合同 $(\operatorname{mod} q)$ ならば，分子もまたこのタイプになる．積のすべての因子は異なる剰余類から来ており，現れてこない剰余類は 0 の類（q の倍数）と，-1 か $+1$ の類だけであるが，-1 と $+1$ の類はともに p では割り切れない．こうして，分母と分子は同じ数の p 因数を持ち，この商は p で割ることはできない．

一方，$z \not\equiv 0, 1 \pmod{q}$ ならば，$(*)$ の分子は $q = p^m$ で割り切れる因子を 1 つ含む．同時に，積にはある 2 つの隣り合った 0 でない剰余類の因子が含まれていないが，そのうちの 1 つは p 因数をまったく含まず，もう 1 つは $q = p^m$ より少ない p 因数を含むことになる．それゆえ，分母より分子の方が p 因数を多く含んでおり，商は p で割り切れる．□

今度は，ほとんど直交するベクトルをまったく含まない任意の部分集合 $Q' \subseteq Q$ を考える．Q' が「小さく」なることを確かめたい．

主張 1． $\boldsymbol{x}, \boldsymbol{y}$ **が** Q **の異なるベクトルなら，**$\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + 2)$ **は**

$$-(q-2) \quad \leq \quad \tfrac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + 2) \quad \leq \quad q-1$$

の範囲にある整数である．

$\boldsymbol{x}$ と $\boldsymbol{y}$ はともに偶数個の成分が -1 となっており，$\boldsymbol{x}$ と $\boldsymbol{y}$ の同じでない成分の数も偶数になる．こうして，すべての $\boldsymbol{x}, \boldsymbol{y} \in Q$ に対して

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle \;=\; (4q-2) \;-\; 2\#\{i : x_i \neq y_i\} \;\equiv\; -2 \pmod{4}$$

となる．つまり，$\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + 2)$ は整数である．

$\boldsymbol{x}, \boldsymbol{y} \in \{+1, -1\}^{4q-2}$ から，$-(4q-2) \leq \langle \boldsymbol{x}, \boldsymbol{y} \rangle \leq 4q-2$ であることがわかり，$-(q-1) \leq \frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + 2) \leq q$ がわかる．下界の等号は成り立たない．というのは，$x_1 = y_1 = 1$ としているので，$\boldsymbol{x} \neq -\boldsymbol{y}$ だからである．上界の等号は $\boldsymbol{x} = \boldsymbol{y}$ のときにだけ成り立つ．

主張 2.　任意の $\boldsymbol{y} \in Q'$ に対して，

$$F_{\boldsymbol{y}}(\boldsymbol{x}) = P\left(\tfrac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + 2)\right) = \binom{\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + 2) - 2}{q-2}$$

で与えられる，n 変数 $x_1, \ldots, x_n$ の $q-2$ 次の多項式は，あらゆる $\boldsymbol{x} \in Q' \backslash \{\boldsymbol{y}\}$ に対して p で割り切れるが，$\boldsymbol{x} = \boldsymbol{y}$ に対しては割り切れない．

2項係数による表示から，$F_{\boldsymbol{y}}(\boldsymbol{x})$ が整数値の多項式であることがわかる．$\boldsymbol{x} = \boldsymbol{y}$ のときは，$F_{\boldsymbol{y}}(\boldsymbol{y}) = 1$ という値になる．$\boldsymbol{x} \neq \boldsymbol{y}$ のときは，補題から，$F_{\boldsymbol{y}}(\boldsymbol{x})$ が p で割り切れないのは，$\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + 2)$ が mod q で 0 か 1 に合同であるとき，かつそのときに限る．主張 1 により，このことが起こるのは，$\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle + 2)$ が 0 か 1 のときだけ，つまり，$\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \{-2, +2\}$ となるときだけである．だから，このとき $\boldsymbol{x}$ と $\boldsymbol{y}$ はほとんど直交することになるが，これは Q' の定義に矛盾する．

主張 3.　以下のようにして得られる，$n-1$ 個の変数 $x_2, \ldots, x_n$ の多項式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ に対しても，同じことが成り立つ．$F_{\boldsymbol{y}}(\boldsymbol{x})$ を単項式に展開し，$x_1 = 1$，さらに $x_i^2 = 1$ $(i > 1)$ という代入によって，変数 x_1 と，他の変数のすべての高次のベキをなくしたものを $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ とする．多項式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ の次数は高々 $q-2$ である．

ベクトル $\boldsymbol{x} \in Q \subseteq \{+1, -1\}^n$ はすべて $x_1 = 1$ と $x_i^2 = 1$ を満たしている．そこで，この代入では集合 Q 上での多項式の値を変えない．また次数も増えないので，$\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ の次数は高々 $q-2$ である．

主張 4.　多項式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ の間には（有理係数の）どんな線形関係も存在しない．つまり，多項式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$，$\boldsymbol{y} \in Q'$ は $\mathbb{Q}$ 上 1 次独立である．とくに，これらの多項式は互いに異なっている．

係数 $\alpha_{\boldsymbol{y}}$ のすべては 0 でないような，$\sum_{\boldsymbol{y} \in Q'} \alpha_{\boldsymbol{y}} \overline{F}_{\boldsymbol{y}}(\boldsymbol{x}) = 0$ という形の関係式があったと仮定する．適当にスカラーを掛ければ，すべての係数は整数だが，すべては p で割り切れないと仮定してもよい．しかしそのとき，あらゆる $\boldsymbol{y} \in Q'$ に対して，$\boldsymbol{x} = \boldsymbol{y}$ での値から $\alpha_{\boldsymbol{y}} \overline{F}_{\boldsymbol{y}}(\boldsymbol{y})$ は p

で割り切れる．それゆえ，$\overline{F}_{\boldsymbol{y}}(\boldsymbol{y})$ は p で割り切れないので，$\alpha_{\boldsymbol{y}}$ は p で割り切れる[2]．

> **主張 5.** $|Q'|$ **は，平方を含まない，高々 $q-2$ 次の $n-1$ 変数単項式の数，つまり，$\sum_{i=0}^{q-2}\binom{n-1}{i}$ で抑えられる．**

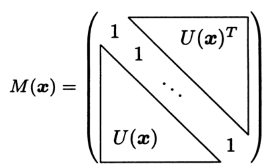
構成から，多項式 $\overline{F}_{\boldsymbol{y}}$ は平方を含まない．そのどの単項式に含まれる変数も，1 次以下だからである．こうして，各 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ は，$n-1$ 個の変数 $x_2,\dots,x_n$ に関する，高々$q-2$ 次の，平方を含まない単項式の 1 次結合である．多項式 $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ は 1 次独立だから，その数 $|Q'|$ は，問題の単項式の数を超えることはできない．

(2) の詳しい証明． $\boldsymbol{x}\boldsymbol{x}^T$ の第 1 列は $\boldsymbol{x}$ そのものである．だから，異なる $\boldsymbol{x}\in Q$ に対しては異なる行列 $M(\boldsymbol{x})=\boldsymbol{x}\boldsymbol{x}^T$ が得られる．これらの行列を，成分が x_ix_j である長さ n^2 のベクトルと考える．簡単な計算

$$\begin{aligned}\langle M(\boldsymbol{x}),M(\boldsymbol{y})\rangle &= \sum_{i=1}^{n}\sum_{j=1}^{n}(x_ix_j)(y_iy_j)\\ &= \Big(\sum_{i=1}^{n}x_iy_i\Big)\Big(\sum_{j=1}^{n}x_jy_j\Big) \;=\; \langle\boldsymbol{x},\boldsymbol{y}\rangle^2 \;\geq\; 4\end{aligned}$$

によって，$M(\boldsymbol{x})$ と $M(\boldsymbol{y})$ のスカラー積が最小となるのは，$\boldsymbol{x},\boldsymbol{y}\in Q$ がほとんど直交するとき，かつそのときに限ることがわかる．

(3) の詳しい証明． $U(\boldsymbol{x})\in\{+1,-1\}^d$ で，$M(\boldsymbol{x})$ のすべての下三角の成分からなるベクトルを表わそう．$M(\boldsymbol{x})=\boldsymbol{x}\boldsymbol{x}^T$ は対称行列で，対角成分の値は $+1$ なので，$M(\boldsymbol{x})\neq M(\boldsymbol{y})$ から $U(\boldsymbol{x})\neq U(\boldsymbol{y})$ が得られる．さらに，



$$4 \;\leq\; \langle M(\boldsymbol{x}),M(\boldsymbol{y})\rangle \;=\; 2\langle U(\boldsymbol{x}),U(\boldsymbol{y})\rangle+n$$

つまり，

$$\langle U(\boldsymbol{x}),U(\boldsymbol{y})\rangle \;\geq\; -\frac{n}{2}+2$$

となり，等号が成り立つのは $\boldsymbol{x}$ と $\boldsymbol{y}$ がほとんど直交するとき，かつそのときに限る．すべてのベクトル $U(\boldsymbol{x})\in S$ は同じ長さ $\sqrt{\langle U(\boldsymbol{x}),U(\boldsymbol{x})\rangle}=$

---

[2] ［訳註］p が素数であることに注意．

$\sqrt{\binom{n}{2}}$ を持つので，点 $U(\boldsymbol{x}), U(\boldsymbol{y}) \in S$ の間の距離が最大となるのは，ちょうど $\boldsymbol{x}$ と $\boldsymbol{y}$ がほとんど直交するときであることがわかる．

(4) の詳しい証明． $q = 9$ のとき $g(9) \approx 758.31$ となり，これは $d+1 = \binom{34}{2} + 1 = 562$ よりも大きい．

大きな d に対する一般的な上界を得るのに，2 項係数の単調性や一山の列であること，また $n! > e(\frac{n}{e})^n$ と $n! < en(\frac{n}{e})^n$ という評価（第 2 章の附録参照）とを使い，

$$\sum_{i=0}^{q-2} \binom{4q-3}{i} < q\binom{4q}{q} = q\,\frac{(4q)!}{q!(3q)!} < q\,\frac{e\,4q\left(\frac{4q}{e}\right)^{4q}}{e\left(\frac{q}{e}\right)^{q} e\left(\frac{3q}{e}\right)^{3q}} = \frac{4q^2}{e}\left(\frac{256}{27}\right)^{q}$$

を導く．こうして，

$$f(d) \;\geq\; g(q) \;=\; \frac{2^{4q-4}}{\sum_{i=0}^{q-2}\binom{4q-3}{i}} \;>\; \frac{e}{64q^2}\left(\frac{27}{16}\right)^{q}$$

という結論が得られる．

このことと，

$$d \;=\; (2q-1)(4q-3) \;=\; 5q^2 + (q-3)(3q-1) \;\geq\; 5q^2 \qquad (q \geq 3),$$

$$q = \tfrac{5}{8} + \sqrt{\tfrac{d}{8} + \tfrac{1}{64}} > \sqrt{\tfrac{d}{8}}, \qquad\qquad \left(\tfrac{27}{16}\right)^{\sqrt{\frac{1}{8}}} > 1.2032$$

とから，十分大きなすべての d に対して，

$$f(d) \;>\; \frac{e}{13d}(1.2032)^{\sqrt{d}} \;>\; (1.2)^{\sqrt{d}}$$

が得られる．□

560 次元の反例は，$q = 9$ に対して商 $g(q) \approx 758$ が次元 $d(q) = 561$ よりもずっと大きいことを注意することによって得られる．このため，$(x_1, x_2, x_3) \neq (1, 1, 1)$ を満たす Q の点によって与えられるような，集合 S の「4 分の 3」だけをとることによって，560 次元の反例が得られている．

ボルスク予想は $d \leq 3$ に対しては成り立つことが知られているが，それより大きな次元では確かめられてこなかった．これと対照的に，上で構成したように（[8] を参照），部分集合 $S \subseteq \{1, -1\}^d$ に制限すれば $d = 8$ までは成り立っている．どちらの場合にも，適当に小さな次元で

反例が発見され得るのは，かなりな程度ありそうなことである．

参考文献

[1] K. ボルスク：「n 次元ユークリッド球面についての 3 つの定理」(*Drei Sätze über die n-dimensionale euklidische Sphäre*), Fundamenta Math. **20** (1933), 177-190.

[2] A. ヒンリクス：「球面コードとボルスク予想」(*Spherical codes and Borsuk's conjecture*), Discrete Math. **243** (2002), 253-256.

[3] J. カーン，G. カライ：「ボルスク予想の反例」(*A counterexample to Borsuk's conjecture*), Bulletin Amer. Math. Soc. **29** (1993), 60-62.

[4] A. ニリー：「ボルスクの問題」(*On Borsuk's problem*), in: "Jerusalem Combinatorics '93" (H. Barcelo and G. Kalai, eds.), Contemporary Mathematics **178**, Amer. Math. Soc. 1994, 209-210.

[5] A. M. ライゴロツキー：「ボルスクの問題における次元について」(*On the dimension in Borsuk's problem*), Russian Math. Surveys (6) **52** (1997), 1324-1325.

[6] O. シュラム：「幅の一定な光る集合」(*Illuminating sets of constant width*), Mathematika **35** (1988), 180-199.

[7] B. ヴァイスバッハ：「大きいボルスク数を持つ集合」(*Sets with large Borsuk number*), Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry **41** (2000), 417-423.

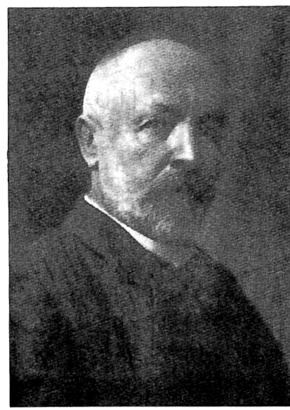
[8] G. M. ツィーグラー：「ハミング・グラフの色つけ，光学的 2 進コード，低次元での 0/1 ボルスク問題」(*Coloring Hamming graphs, optimal binary codes, and the 0/1-Borsuk problem in low dimensions*), Preprint, TU Berlin, June 2000.

解析学



「ヒルベルトの海辺のリゾート・ホテル」

第15章　集合，関数，連続体仮説



ゲオルク・カントール

19世紀後半にゲオルク・カントールによって創られた集合論は，数学を根底から変えてしまった．今日の数学は集合の概念なしに考えることはできないし，ダーフィト・ヒルベルトが述べているように「我々のためにカントールが創ってくれた（集合論の）パラダイスから，誰も我々を追い出すことはできない」のである．

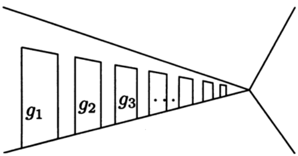
カントールの基本概念の1つは，集合 M の**サイズ**または**濃度**であり，$|M|$ と表わされる．有限集合に関しては難しいことはない．元の数を数えて，M がちょうど n 個の元を含んでいれば，M は n 集合であるとか，サイズが n であるとか言う．こうして，2つの有限集合 M と N は，同じ個数の元を含むとき，同じサイズで，$|M| = |N|$ と書かれる．

この**同じ**サイズの概念を無限集合にまで拡張するために，有限集合に対する示唆に富んだ思考実験を行ってみる．ある数の人がバスに乗っているとする．どんなときに，人の数と座席の数が同じであると言っているのだろうか？ それは簡単で，すべての人に座って貰えばよい．どの人にも座席があり，空いた席がないのなら，そしてそのときにのみ，(人と座席の) 2つの集合は同じ数ということになる．言い換えれば，一方の集合から他方の集合への**全単射**が存在すれば，この2つのサイズは同じである．

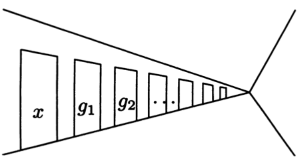
そこでこれを定義にする．つまり，(有限であれ無限であれ) 2つの任意の集合 M と N が**同じサイズ**または**同じ濃度**であると言うのは，M から N への全単射があるとき，かつそのときに限る．明らかに，サイズが同じというこの概念は同値関係であり，サイズが同じ集合の作るあらゆる類に**濃度**と呼ばれる数を対応させることができる．たとえば，有

限集合に対しては $0, 1, 2, \ldots, n, \ldots$ という濃度が得られる．ここで，n は n 集合の類を表しており，とくに，0 は**空集合** $\varnothing$ を表している．さらに，有限集合 M の真部分集合は M よりサイズが小さいという当たり前な事実を見ておくことにする．

無限集合に目を向けると，理論は非常に興味深いものに（そして高度に非直観的なものに）なる．自然数の集合 $\mathbb{N} = \{1, 2, 3, \ldots\}$ を考える．$\mathbb{N}$ と 1 対 1 対応をつけられるとき，集合 M を**可算**と言う．言い換えれば，M の元を $m_1, m_2, m_3, \ldots$ のように数え上げられるなら，M は可算集合である．しかしここで，奇妙なことが起こる．$\mathbb{N}$ に新しい元 x を付け加えたとする．すると，$\mathbb{N} \cup \{x\}$ もまた可算で，それゆえ，$\mathbb{N}$ と同じサイズなのである！



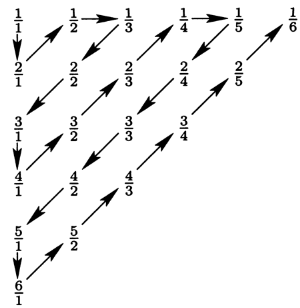
このことには「ヒルベルトのホテル」という楽しい説明がある．ホテルの部屋が可算個あって，$1, 2, 3, \ldots$ と番号がついている．そして i 号室には顧客 g_i が入っている，つまり．ホテルは満室であるとする．そこへ，新しい客 x が泊まりにやって来ると，ホテルの支配人は「申し訳ありませんが，満室でございます」と答えることになる．「大丈夫ですよ」と新来の客が言う．「g_1 というお客さんを 2 号室に移し，g_2 さんを 3 号室に，g_3 さんを 4 号室に，というように移して，私は 1 号室に泊まります.」支配人は驚いたが（彼は数学者でなかったのだ），これはうまくいった．すべてのお客に新しく来た客 x も泊めることができたのだ．



これで，もう 1 人の客 y が来ても，もう 1 人の z が来ても，また何人でも泊めることができるのだ．特に注意すべきことは，有限集合の場合と違って，**無限**集合 M のある真部分集合が M と同じサイズを持つことも起こり得るということである．実際，容易にわかるように，これが無限であることの特徴付けなのである．つまり，集合が無限であるのは，同じサイズの真部分集合を持つとき，かつそのときに限るのである．

ヒルベルトのホテルを忘れて，馴染み深い数の集合を取り上げよう．整数の集合 $\mathbb{Z}$ もまた可算である．というのは，$\mathbb{Z}$ を $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ の形に数え上げることができるからである．多分もっと驚くだろうが，有理数の集合 $\mathbb{Q}$ もまた可算である．正の有理数の集合 $\mathbb{Q}^+$ を図に示したように数えていけば（すでに出てきた数は数えないで），$\mathbb{Q}^+$ が可算集合であることがわかり，それゆえ $\mathbb{Q}$ も可算集合であることがわかる．最初に 0 を数え，$\frac{p}{q}$ のすぐあとに $-\frac{p}{q}$ を数えるのである．この数え方だと，

$$\mathbb{Q} = \{0, 1, -1, 2, -2, \tfrac{1}{2}, -\tfrac{1}{2}, \tfrac{1}{3}, -\tfrac{1}{3}, 3, -3, 4, -4, \tfrac{3}{2}, -\tfrac{3}{2}, \dots\}$$



となる．この図を使って次の主張を説明することもできる．

可算個の可算集合 M_n の和集合はまた可算である．

実際，$M_n = \{a_{n1}, a_{n2}, a_{n3}, \dots\}$ とおき，上と同じように

$$\bigcup_{n=1}^{\infty} M_n = \{a_{11}, a_{21}, a_{12}, a_{13}, a_{22}, a_{31}, a_{41}, a_{32}, a_{23}, a_{14}, \dots\}$$

と数える．

実数 $\mathbb{R}$ はどうだろうか？ まだ可算だろうか？ いやそうではない．そして，このことを示す「カントールの**対角線論法**」は集合論全体に対して基本的な重要性を持っているだけでなく，希有(けう)な天才的閃(ひらめ)きとして天書に載るべきものである．

定理 1．実数の集合 $\mathbb{R}$ は非可算である．

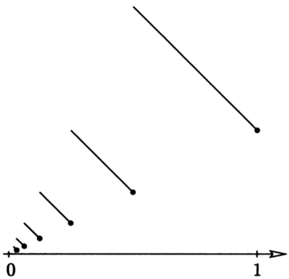
■ **証明．** 可算集合 $M = \{m_1, m_2, m_3, \dots\}$ のどんな部分集合 N も**高々可算**（つまり，有限かまたは可算）である．実際，N の元を M で数えるように数えればよい．したがって，もし $\mathbb{R}$ の非可算な部分集合を見つけることができたら，なおのこと $\mathbb{R}$ は可算ではあり得ないのである．調べようと思う $\mathbb{R}$ の部分集合 M は，$0 < r \leq 1$ を満たすすべての正の実数 r のなす区間 $(0, 1]$ である．示したいこととは逆に，M が可算であると仮定し，M を $M = \{r_1, r_2, r_3, \dots\}$ と数え上げたとする．r_n を，終わりに 0 が無限に並ぶことのないようにして，一意的な無限小数展開

$$r_n = 0.a_{n1}a_{n2}a_{n3}\cdots$$

をしておく．ここで，すべての n と i に対して $a_{ni} \in \{0, 1, \dots, 9\}$ である．たとえば，$0.7 = 0.6999\cdots$ とする．今度は 2 重に無限の配列

$$\begin{aligned} r_1 &= 0.a_{11}a_{12}a_{13}\cdots \\ r_2 &= 0.a_{21}a_{22}a_{23}\cdots \\ \vdots\ &\quad \vdots \\ r_n &= 0.a_{n1}a_{n2}a_{n3}\cdots \\ \vdots\ &\quad \vdots \end{aligned}$$

を考える．あらゆる n に対して，a_{nn} と異なる $b_n \in \{1,\ldots,8\}$ を選ぶ．明らかにこれはいつでもできる．そのとき，$b = 0.b_1b_2b_3\cdots b_n\cdots$ は考えている集合 M の中の実数であり，それゆえ何番目かになっていなければならず，たとえば $b = r_k$ となっている．しかし，これはあり得ない．なぜなら，b_k は a_{kk} と異なっているからである．これが証明のすべてである．□



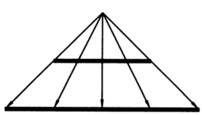
$f:(0,1] \longrightarrow (0,1)$.

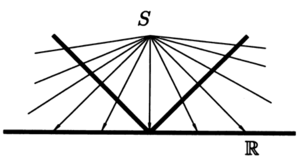
もう少し実数の話をしよう．4 つのタイプの区間 $(0,1), (0,1], [0,1), [0,1]$ はすべて同じサイズであることに注意する．たとえば，$(0,1]$ と $(0,1)$ が同じ濃度を持つことを確かめるためには，

$$y = \begin{cases} \frac{3}{2} - x & (\frac{1}{2} < x \le 1 \text{ のとき}) \\ \frac{3}{4} - x & (\frac{1}{4} < x \le \frac{1}{2} \text{ のとき}) \\ \frac{3}{8} - x & (\frac{1}{8} < x \le \frac{1}{4} \text{ のとき}) \\ \quad\vdots & \end{cases}$$

で定義される写像 $f:(0,1] \longrightarrow (0,1), x \longmapsto y$ を使えばよい．実際，この写像は全単射である．なぜなら，第 1 行の y の領域は $\frac{1}{2} \le y < 1$ であり，第 2 行は $\frac{1}{4} \le y < \frac{1}{2}$ であり，第 3 行は $\frac{1}{8} \le y < \frac{1}{4}$ であり，などとなっている．

次に，（有限の長さ > 0 の）どんな 2 区間も，図にあるような中心射影を考えれば，同じサイズであることがわかる．それ以上のこともわかる．つまり，あらゆる（長さが > 0 の）区間は実数直線 $\mathbb{R}$ 全体と同じサイズを持つ．これを見るには，開区間 $(0,1)$ を折り曲げて，中心 S から $\mathbb{R}$ の上へ射影すればよい．





それで，結論としては，長さが > 0 であるどんな開，半開，閉区間（有限でも無限でも）も同じサイズを持っていることになる．このサイズを c と書く．c は**連続体** (continuum) を意味している（この名前は区間 $[0,1]$ に対して使われることがある）．

有限と無限の区間が同じサイズであるということはよく考えれば思い付くかも知れないが，真っ向から直観に逆らう事実がある．

定理 2．実数のすべての順序対の集合 $\mathbb{R}^2$（つまり，実平面）は $\mathbb{R}$ と同じサイズを持つ．

■ **証明．** これを見るには，すべての対 (x,y)，$0 < x,y \le 1$ の集合を

$(0,1]$ の上に全単射として写すことができることを証明すればよい．これもまた天書の証明である．対 (x,y) をとり，x,y を，次の例のように，途中で終わらないような一意的な小数に展開して書く．

$$\begin{array}{rclllllll} x &=& 0.3 & 01 & 2 & 007 & 08 & \cdots \\ y &=& 0.009 & 2 & 05 & 1 & 0008 & \cdots \end{array}$$

ここで，x と y の数字が，次の 0 でない数字までのグループに分けられていることに注意する．そこで，(x,y) に対して，数 $z \in (0,1]$ を次のようにして対応させる．x の最初のグループを書き，そのあとに y の最初のグループを，次に x の 2 番目のグループを，というように書いて行く．すると，上の例では

$$z = 0.3\ 009\ 01\ 2\ 2\ 05\ 007\ 1\ 08\ 0008\ \cdots$$

となる．x も y もあるところから先が 0 だけということはないので，z に対する表示もまた途中で終わらない小数展開になっている．逆に z の表示から原像 (x,y) を直ちに読み取ることができるので，この写像は全単射である．これで証明は終わり．　□

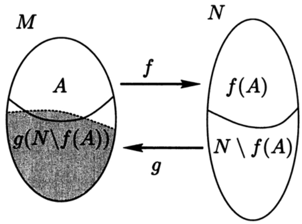
$(x,y) \longmapsto x+iy$ は $\mathbb{R}^2$ から複素数 $\mathbb{C}$ の上への全単射だから，$|\mathbb{C}| = |\mathbb{R}| = c$ という結論になる．なぜ，$|\mathbb{R}^2| = |\mathbb{R}|$ という結果がそれほど予期されないのだろうか？　なぜなら，これは**次元**についての我々の直観に反するからである．それは，2 次元平面 $\mathbb{R}^2$（そして，帰納法により，一般に n 次元空間 $\mathbb{R}^n$）が，1 次元の直線 $\mathbb{R}$ の上に全単射に写され得るということを言っているのである．こうして，次元というものは一般には全単射な写像によっては保存されないのである．しかしながら，もしその写像と逆写像が連続であることを要求するなら，次元は保存される．これを最初に示したのはブラウエルである．

もう少し進んでみよう．これまでに，サイズが同じという概念を考えた．どんなときに，M が高々 N と同じ大きさであると言うことにしようか？　ここでも写像が鍵になる．$|M| = \mathbf{m}$, $|N| = \mathbf{n}$ である集合 M と N に対して，M から N への**単射**が存在するとき，濃度 $\mathbf{m}$ は濃度 $\mathbf{n}$ **以下**であると言う．明らかに，$\mathbf{m} \leq \mathbf{n}$ という関係は，代表集合 M, N の選び方によらない．有限集合に対しては，これは我々の直観的な概念に対応している．ある m 集合がある n 集合と高々同じ大きさであるのは，

$m \leq n$ のとき，かつそのときに限る．

ここに，基本的な問題がある．確かに，不等式に関する普通の規則が濃度に対しても成り立って欲しいと思うだろう．しかし，無限の濃度に対しても成り立つだろうか？ とくに，$\mathfrak{m} \leq \mathfrak{n}$, $\mathfrak{n} \leq \mathfrak{m}$ から $\mathfrak{m} = \mathfrak{n}$ が得られるというのは本当だろうか？ 答えは肯定的で，有名なシュレーダー–ベルンシュタインの定理[1]が成り立つ．以下にあげた証明は，アンドレイ・ゼレヴィンスキーから習ったものだが，紛れもなく 1 つの宝石である．

定理 3. **2 つの集合 M と N がそれぞれ相手の中に単射に写像することが可能であれば，M から N への全単射が存在し，$|M| = |N|$ となる．**

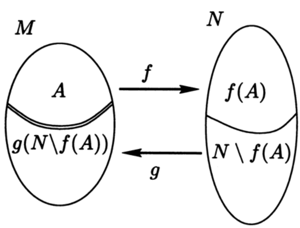


■ **証明．** $f : M \longrightarrow N$ と $g : N \longrightarrow M$ を単射とする．各 $A \subseteq M$ に対して，集合 $F(A) \subseteq M$ を

$$F(A) \ = \ M \setminus g(N \setminus f(A))$$

と定義する．つまり，任意の部分集合 $A \subseteq M$ は $f(A) \subseteq N$ に写され，N におけるその補集合 $N \setminus f(A)$ をとる．この補集合を g で戻して $g(N \setminus f(A)) \subseteq M$ を作り，最後に M におけるその補集合をとるのである（余白の図を参照のこと）．

ここで，$F(A_0) = A_0$ を満たす部分集合 A_0 があったとする．つまり，$g(N \setminus f(A_0)) = M \setminus A_0$ であるとする．すると，明らかに，



$$\phi(x) \ = \ \begin{cases} f(x) & (x \in A_0 \text{のとき}), \\ g^{-1}(x) & (x \notin A_0 \text{のとき}) \end{cases}$$

とおけば，M から N への全単射になる．それゆえあとは，このような「固定される集合」A_0 を見つけるだけである．これを見つける方法は次の観察に基づいている．

主張． $A_1, A_2, A_3, \ldots$ **を** M **の任意の集合族とすると，**

$$F(\bigcap_{i \geq 1} A_i) \ = \ \bigcap_{i \geq 1} F(A_i)$$

となる．

---

[1] ［訳註］カントール–ベルンシュタインの定理と言われることも多い．

これを見るために，まず (i) $f(\bigcap A_i) = \bigcap f(A_i)$ に注意する．これは f が単射だからである．次に (ii) $g(\bigcup B_i) = \bigcup g(B_i)$ という事実も使う．これは任意の写像 $g : N \longrightarrow M$ と任意の集合 $B_i \subseteq N$ に対して成り立っている．すると，

$$
\begin{aligned}
F(\bigcap A_i) &= M \setminus g(N \setminus f(\bigcap A_i)) \\
&= M \setminus g(N \setminus \bigcap f(A_i)) && \text{(i) による} \\
&= M \setminus g(\bigcup (N \setminus f(A_i))) && \text{ド・モルガンの法則による} \\
&= M \setminus (\bigcup g(N \setminus f(A_i))) && \text{(ii) による} \\
&= \bigcap (M \setminus g(N \setminus f(A_i))) && \text{ド・モルガンの法則による} \\
&= \bigcap F(A_i)
\end{aligned}
$$

となり，主張が示される．今度は部分集合の鎖

$$M \ \supseteq\ F(M)\ \supseteq\ F^2(M)\ \supseteq\ F^3(M)\cdots$$

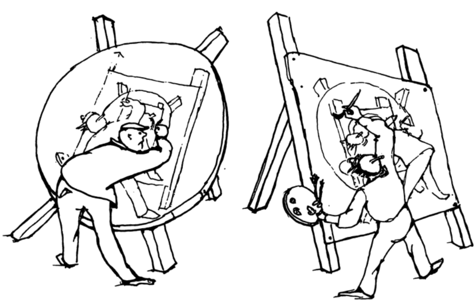
を考え，この鎖のすべての集合の共通部分として A_0 を

$$A_0 \ = \ M \cap F(M) \cap F^2(M) \cap F^3(M)\cdots$$

と定義する．これと主張から

$$F(A_0) \ = \ F(M) \cap F^2(M) \cap F^3(M)\cdots$$

が得られ，つまり，$F(A_0) = A_0$ となる．見つかった！ □



「シュレーダー–ベルンシュタイン画法」



「最小の無限濃度」

不等式を統制する他の関係はどうだろうか？ 普通そうであるように，$\mathfrak{m} \leq \mathfrak{n}$ だが $\mathfrak{m} \neq \mathfrak{n}$ であるときに，$\mathfrak{m} < \mathfrak{n}$ とおく．どんな2つの濃度 $\mathfrak{m}$ と $\mathfrak{n}$ に対しても，3つの可能性

$$\mathfrak{m} < \mathfrak{n},\ \mathfrak{m} = \mathfrak{n},\ \mathfrak{m} > \mathfrak{n}$$

のうちの高々1つが成り立つことがわかるし，濃度の理論から，実際にこのうち1つの関係だけが成り立つこともわかる（本章の附録，命題2を参照）．さらに，シュレーダー–ベルンシュタインの定理から，関係 $<$ が推移的であることが得られる．つまり，$\mathfrak{m} < \mathfrak{n}$ と $\mathfrak{n} < \mathfrak{p}$ とから $\mathfrak{m} < \mathfrak{p}$ が得られるのである．こうして，濃度は有限濃度 $0, 1, 2, 3, \ldots$ から始まって，線形順序に並んでいる．通常のツェルメロ–フレンケルの公理系（とくに選択公理）に訴えれば，任意の無限集合 M が可算集合を含んでいることがわかる．実際，M は元を1つは含んでいるので，それを m_1 とする．集合 $M \setminus \{m_1\}$ は空でなく（無限集合だから），それゆえある元 m_2 を含んでいる．$M \setminus \{m_1, m_2\}$ を考えて，m_3 の存在が推論され，さらに次々とすればよい．だから，可算集合のサイズは**最小の無限**濃度であって，$\aleph_0$ と書かれる（「アレフ・ゼロ」と発音する）．

任意の無限濃度 $\mathfrak{m}$ に対して $\aleph_0 \leq \mathfrak{m}$ となることの系として，直ちに任意の無限濃度 $\mathfrak{m}$ に対する「ヒルベルトのホテル」を，つまり，任意の無限集合 M に対して $|M \cup \{x\}| = |M|$ であることを証明することができる．実際，M は部分集合 $N = \{m_1, m_2, m_3, \ldots\}$ を含んでいる．そこで，x を m_1 に，m_1 を m_2 になどと写し，$M \backslash N$ の元は動かさない．これが求めていた全単射である．

これによって，以前に述べるだけだった次の結果の証明もしたことになる．

あらゆる無限集合は同じサイズの真部分集合を持つ．

これまでのところ，濃度 $0, 1, 2, \ldots, \aleph_0$ と，さらに $\aleph_0$ より大きな $\mathbb{R}$ の濃度 c を知っている．$|\mathbb{Q}| = \aleph_0$ である $\mathbb{Q}$ は，$|\mathbb{R}| = c$ である $\mathbb{R}$ に広がることから，すぐに次の問題を思い付く．

$c = |\mathbb{R}|$ は $\aleph_0$ の次の無限濃度か？

するともちろん，次に大きな濃度が**存在**するかどうかが問題になる．つまり，$\aleph_1$ に意味があるかどうかである．それは存在する．その証明は本章の附録で大筋を述べておく．

$c = \aleph_1$ という主張は**連続体仮説**として知られている．連続体仮説が正しいかどうかという問題は，数十年にわたって，全数学でも最高度な挑戦の1つであり続けた．解答は最終的にクルト・ゲーデルとポール・

コーエンによって与えられたが，それは論理的思考の限界というものを教えてくれるものとなった．彼らは，$c=\aleph_1$ という主張がツェルメロ–フレンケルの公理系と独立であることを示した．それは，平行線の公理が，ユークリッド幾何の他の公理と独立であるのと同じである．$c=\aleph_1$ が成り立つモデルも存在するし，$c\neq\aleph_1$ が成り立つような集合論のモデルも存在する．

この事実を考慮すると，連続体仮説と同値な（たとえば解析学での）他の条件があるかどうかを問題にすることはとても興味深い．以下で，そのような1つの例とポール・エルデシュによるきわめてエレガントで単純な解答を述べてみたい．1962年にウェツェルは次のことを問題にした．

$\{f_\alpha\}$ を複素数上の互いに異なる解析関数族で，各 $z\in\mathbb{C}$ に対して値の集合 $\{f_\alpha(z)\}$ が可算であるとする．この性質を (P_0) と呼ぼう．そのとき，この族自身も可算であることになるか？

その直後，エルデシュは，驚くべきことに，答が連続体仮説によることを示した．

定理 4. **$c>\aleph_1$ であれば，(P_0) を満たすあらゆる族 $\{f_\alpha\}$ は可算である．一方，$c=\aleph_1$ であれば，サイズが c の，(P_0) を満たすある族 $\{f_\alpha\}$ が存在する．**

証明するには，濃度と順序数に関するいくつかの基本的事実が必要となる．これらの概念に馴染みのない読者のために，本章の附録に必要なすべての結果をまとめておいた．

■ **定理 4 の証明.** まず $c>\aleph_1$ と仮定する．サイズ $\aleph_1$ のどんな解析関数族 $\{f_\alpha\}$ に対しても，ある複素数 z_0 が存在して，すべての $\aleph_1$ 個の値 $f_\alpha(z_0)$ が異なっていることを示そう．その結果，関数族が (P_0) を満たせば可算でなくてはならないことになる．

これを見るために，順序数に関する知識を使う．まず，$\aleph_1$ の最初の順序数 ω_1 に従って，族 $\{f_\alpha\}$ を整列させる．これはつまり，附録の命題 1 によって，添え字集合が ω_1 より小さいすべての順序数 α を走るということである．次に，対 (α,β), $\alpha<\beta<\omega_1$ の集合のサイズが $\aleph_1$ であることを示す．任意の $\beta<\omega_1$ は可算順序数なので，そのような β を固定すると，対 (α,β), $\alpha<\beta$ の集合は可算となる．すべての $\aleph_1$ 個の β に

わたって和をとれば，附録の命題 6 によって，すべての対 (α, β), $\alpha < \beta$ の集合のサイズは $\aleph_1$ である．

さて，任意の対 $\alpha < \beta$ に対して，集合

$$S(\alpha, \beta) \ = \ \{z \in \mathbb{C} : f_\alpha(z) = f_\beta(z)\}$$

を考える．各集合 $S(\alpha, \beta)$ が可算であることが言える．これを示すために，複素平面の，原点を中心とする半径 $k = 1, 2, 3, \ldots$ の円 C_k を考える．f_α と f_β がある C_k の中の無限個の点で一致すれば，解析関数に関するよく知られた定理によって，f_α と f_β は一致する．それゆえ，各 C_k の上では有限個の点でしか一致できないので，全部合わせても高々可算個の点でしか一致しない．そこで，$S = \bigcup_{\alpha<\beta} S(\alpha, \beta)$ とおく．各集合 $S(\alpha, \beta)$ は可算だから，また命題 6 により，S はサイズ $\aleph_1$ である．そしてここが証明のさわりである．知っているように $\mathbb{C}$ のサイズは c であり，仮定により c は $\aleph_1$ より大きいのだから，S に属さない複素数 z_0 があって，この z_0 に対して，$\aleph_1$ 個の値 $f_\alpha(z_0)$ はすべて異なっている．

次に $c = \aleph_1$ と仮定する．実部と虚部が有理数である複素数 $p + iq$ の作る集合 $D \subseteq \mathbb{C}$ を考える．各 p に対して集合 $\{p + iq : q \in \mathbb{Q}\}$ は可算だから，D が可算であることがわかる．さらに，D は $\mathbb{C}$ の中で**稠密**である．つまり，複素平面の任意の開円盤は D のある点を含む．$\{z_\alpha : 0 \leq \alpha < \omega_1\}$ は $\mathbb{C}$ を整列させたものとする．そこで，$\aleph_1$ 個の互いに異なる解析関数族 $\{f_\beta : 0 \leq \beta < \omega_1\}$ で，

$$f_\beta(z_\alpha) \in D \quad (\alpha < \beta \text{である限り}) \tag{1}$$

であるようなものを構成する．そのような関数族は条件 (P_0) を満たす．実際，各点 $z \in \mathbb{C}$ にはある添え字があり，たとえば，$z = z_\alpha$ となっている．すると，すべての $\beta > \alpha$ に対して，値 $\{f_\beta(z_\alpha)\}$ は**可算**集合 D の中にある．α は可算順序数だから，$\beta \leq \alpha$ であるような関数 f_β は高々可算個の値 $f_\beta(z_\alpha)$ しか追加しない．それで，すべての値の集合 $\{f_\beta(z)\}$ は同じように高々可算である．それゆえ，もし (1) を満たす族 $\{f_\beta\}$ を構成できたなら，定理の第 2 の部分の証明が終わる．

$\{f_\beta\}$ の構成は超限帰納法による．f_0 としてはどんな解析関数をとってもよく，たとえば,「f_0 = 定数」ととる．すべての $\beta < \gamma$ に対して，f_β がすでに構成されていると仮定する．γ は可算順序数だから，

$\{f_\beta : 0 \leq \beta < \gamma\}$ を並べ直して，$g_1, g_2, g_3, \ldots$ という列にすることができる．$\{z_\alpha : 0 \leq \alpha < \gamma\}$ に同じ並べ直しをすれば，$w_1, w_2, w_3, \ldots$ という列が得られる．そこで，関数 f_γ を，各 n に対して

$$f_\gamma(w_n) \in D \qquad \text{かつ} \qquad f_\gamma(w_n) \neq g_n(w_n) \tag{2}$$

という条件を満たすように作るのである．2 番目の条件は，すべての関数 f_γ $(0 \leq \gamma < \omega_1)$ が互いに異なっていることを保証し，最初の条件は (1) そのものであり，上での議論により，(P_0) を導く．$f_\gamma(w_n) \neq g_n(w_n)$ という条件がまたも対角線論法であることに注意する．

f_γ を構成するために

$$\begin{aligned} f_\gamma(z) = \varepsilon_0 + \varepsilon_1(z - w_1) + \varepsilon_2(z - w_1)(z - w_2) \\ + \varepsilon_3(z - w_1)(z - w_2)(z - w_3) + \cdots \end{aligned}$$

と書く．γ が有限順序数なら，f_γ は多項式で，それゆえ解析的であり，確かに (2) を満たすように数 ε_i を選ぶことができる．今度は γ が可算順序数とすると，

$$f_\gamma(z) \quad = \quad \sum_{n=0}^{\infty} \varepsilon_n (z - w_1) \cdots (z - w_n) \tag{3}$$

となる．ε_m $(m \geq n)$ の値は，値 $f_\gamma(w_n)$ には何の影響も及ぼさないので，ε_n を一歩ずつ選んで行くことができる．もし列 (ε_n) が十分速く 0 に収束するなら，(3) はある解析関数を定める．最後に，集合 D は稠密なので，f_γ が (2) の要請を満たすように，この列 (ε_n) を選ぶことができる．これで証明は終わりである． □

附録：濃度と順序数

最初に，各濃度に対し，その次に大きな濃度があるかという問題を考えよう．その初めとして，あらゆる濃度 $\mathbf{m}$ に対し，常に $\mathbf{m}$ より大きな濃度 $\mathbf{n}$ が存在することを示す．このためにまた，カントールの対角線論法を変形したものを使う．

M を集合とすれば，M のすべての部分集合の作る集合 $\mathcal{P}(M)$ は M より大きなサイズである．$m \in M$ に $\{m\} \in \mathcal{P}(M)$ を対応させれば，



「伝説の語るところによれば，海辺を歩きながら無限について瞑想をしていた聖アウグスティヌスは，小さな貝殻で大海の水を汲み出そうとする子供を見た ... 」

M が $\mathcal{P}$ のある部分集合の上に全単射に写されることがわかるので，定義により $|M| \leq |\mathcal{P}(M)|$ である．残っているのは，$\mathcal{P}(M)$ が M のある部分集合の上には全単射に写すことができないことを示すことである．反対に，$N \subseteq M$ から $\mathcal{P}(M)$ の上への全単射 $\varphi : N \longrightarrow \mathcal{P}(M)$ があったとしよう．φ による像に含まれないような N の元の集合，つまり $U = \{m \in N : m \notin \varphi(m)\}$ を考えよう．φ は全単射だから，$\varphi(u) = U$ であるような $u \in N$ が存在する．すると，$u \in U$ か $u \notin U$ であるが，どちらの選択肢も不可能である！ 実際，$u \in U$ なら，U の定義により，$u \notin \varphi(u) = U$ であり，$u \notin U = \varphi(u)$ なら $u \in U$ となる．矛盾である．

おそらく，読者はこれまでにこの議論に出会っているだろう．昔からある理髪師の謎々である.「理髪師は自分の髭を剃らないすべての人の髭を剃る人である．理髪師は自分の髭を剃るだろうか？」

この先の理論に進むために，もう 1 つのカントールの偉大な概念である，順序集合と順序数を導入する．集合 M が $<$ によって**順序付け**られているとは，関係 $<$ が推移的で，M の任意の異なる 2 元 a と b に対して，$a < b$ か $b < a$ かが起こるときに言う．たとえば，$\mathbb{N}$ は，大きさに従って通常のように順序付け，$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ とすることができるが，もちろん $\mathbb{N}$ を逆向きに順序付けて $\mathbb{N} = \{\ldots, 4, 3, 2, 1\}$ とすることも，奇数を数えたあとで偶数を数えることにして $\mathbb{N} = \{1, 3, 5, \ldots, 2, 4, 6, \ldots\}$ とすることもできる．

ここに発展性のある概念がある．順序集合 M が**整列**しているとは，M のあらゆる空でない部分集合に最初の元が存在するときに言う．このように，上の $\mathbb{N}$ の 1 番目と 3 番目の順序は整列順序だが，2 番目の順序は整列順序ではない．ここで,（選択公理を含む）公理から導かれる基本的な**整列定理**が成り立ち，それは，**あらゆる**集合 M は整列させることができるというものである．以下では，整列させられている集合だけを扱うことにする．

整列集合 $\mathbb{N} = \{1, 2, 3, \ldots\}$ と $\mathbb{N} = \{1, 3, 5, \ldots, 2, 4, 6, \ldots\}$ は相似ではない．前の順序では直前の元を持たない元はただ 1 つなのに，あとの順序では 2 つある．

2 つの整列集合 M と N が**相似**（または**同じ順序型**）であるとは，M から N の上への順序を保つ全単射 φ が存在するときに言う．つまり，$m <_M n$ のとき $\varphi(m) <_N \varphi(n)$ となるとしている．ある整列集合と相似な順序集合は，それ自身整列集合であることに注意する．

明らかに，相似性は同値関係であり，同値な集合の類に属するものとして**順序数** α を述べることができる．有限集合に対しては，任意の 2 つの順序は相似な整列順序であり，n 集合の類に対しては，また順序数 n

を使うことができる．定義により，2 つの相似な集合は同じ濃度を持つ．それゆえ，順序数 α の**濃度** $|\alpha|$ という言い方にも意味がある．さらに，ある整列集合の部分集合も，そこへ制限した順序に関して整列集合になっていることに注意する．

濃度に対してしたように，今度は順序数を比べよう．M を整列集合，$m \in M$ のとき，$M_m = \{x \in M : x < m\}$ を，m によって定まる M の（**初期**）**切片**と言う．N が M の切片であるのは，ある m に対して $N = M_m$ となっているときである．だから特に，m が M の最初の元ならば，M_m は空集合である．今度は，μ と ν を整列集合 M と N の順序数とする．M が N の切片と相似のとき，μ は ν より小さい，$\mu < \nu$ と言う．ここでも，$\mu < \nu, \nu < \pi$ から $\mu < \pi$ が得られるという推移律が成り立つ．なぜなら，相似を与える写像は切片を切片の上に写すからである．

$\{1, 2, 3, \ldots\}$ の順序数は $\{1, 3, 5, \ldots, 2, 4, 6, \ldots\}$ の順序数より小さい．

明らかに，有限集合に対しては，$m < n$ は通常の意味と対応している．大きさによって並べられた $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ の順序数を ω と書く．任意の有限の n に対しては，切片 $\mathbb{N}_{n+1}$ を考えることによって，$n < \omega$ であることがわかる．次に，どんな無限順序数 α に対しても，$\omega \leq \alpha$ であることがわかる．実際，無限整列集合 M が順序数 α を持てば，M は最初の元 m_1 を含み，集合 $M \backslash m_1$ は最初の元 m_2 を含み，集合 $M \backslash \{m_1, m_2\}$ は最初の元 m_3 を含む．これを続けて行けば，M の列 $m_1 < m_2 < m_3 < \cdots$ が得られる．$M = \{m_1, m_2, m_3, \ldots\}$ であれば，M は $\mathbb{N}$ に相似で，$\alpha = \omega$ となる．一方，$M \backslash \{m_1, m_2, \ldots\}$ が空でなければ，それは最初の元 m を含み，$\mathbb{N}$ は切片 M_m と相似であり，つまり定義により，$\omega < \alpha$ であるという結論が得られる．

さて，順序数に関する 3 つの基本的な結果を述べよう（証明は与えないが，難しいわけではない）．第 1 のものは，任意の順序数 μ には「標準的な」代表元である整列集合 W_μ があるというものである．

命題 1. μ **を順序数，** W_μ **を** μ **より小さな順序数の集合とすると，以下が成り立つ．**

(i) W_μ **の元は互いに比較することができる．**

(ii) W_μ **を大きさで並べると，** W_μ **は整列集合で，その順序数は** μ **である．**

命題 2. **任意の 2 つの順序数 μ と ν は，関係 $\mu < \nu$, $\mu = \nu$, $\mu > \nu$ のどれか 1 つを満たす.**

命題 3. **順序数のなす集合は（大きさで並べれば）整列集合である.**

順序数の世界へ旅していたが，濃度の世界に戻ることにしよう．$\mathfrak{m}$ を濃度とし，$|\mu| = \mathfrak{m}$ を満たすすべての順序数 μ の集合を $O_\mathfrak{m}$ と書く．命題 3 によって，$O_\mathfrak{m}$ には最小の順序数 $\omega_\mathfrak{m}$ が存在する．それを $\mathfrak{m}$ の**最初の順序数**と言う．たとえば，ω は $\aleph_0$ の最初の順序数である．

準備ができたので，本章に対する基本的事実を証明することにしよう．

命題 4. **あらゆる濃度 $\mathfrak{m}$ に対して，その次に大きな濃度が明確に存在する.**

■ **証明.** 何かより大きな濃度 $\mathfrak{n}$ が存在することはすでに知っている．$\mathfrak{m}$ より大きく，高々 $\mathfrak{n}$ の大きさのすべての濃度の作る集合 $\mathcal{K}$ を考える．各 $\mathfrak{p} \in \mathcal{K}$ に対して，その最初の順序数 $\omega_\mathfrak{p}$ を対応させる．これら最初の順序数の中で最小のものが存在し（命題 3），それに対応する濃度は $\mathcal{K}$ の中で最小であり，よって $\mathfrak{m}$ の次に大きい濃度になっている．これが欲しかったことである． □

命題 5. **無限集合 M の濃度が $\mathfrak{m}$ で，M を最初の順序数 $\omega_\mathfrak{m}$ に従って整列させると，M には最終元が存在しない.**

■ **証明.** 実際，M に最終元 m が存在すれば，切片 M_m の順序数は $\mu < \omega_\mathfrak{m}$ で，$|\mu| = \mathfrak{m}$ である．これは $\omega_\mathfrak{m}$ の定義に矛盾する． □

最終的に必要となるのは，可算集合の可算和が可算であることよりかなり強い結果である．以下の結果では，可算集合の**任意の族**を考えている．

命題 6. **$\mathfrak{m}$ を無限濃度とし，$\{A_\alpha\}$ を可算集合 A_α のサイズ $\mathfrak{m}$ の族であるとすると，和集合 $\bigcup_\alpha A_\alpha$ のサイズは高々 $\mathfrak{m}$ である.**

■ **証明.** 集合 A_α は互いには異なると仮定してよい．こうしても，和集合のサイズがより大きくなることがあるだけである．M ($|M| = \mathfrak{m}$) を添え字集合とし，最初の順序数 $\omega_\mathfrak{m}$ に従って整列させておく．各 $\alpha \in M$ を，ω に従って並べた可算集合 $B_\alpha = \{b_{\alpha 1 = \alpha}, b_{\alpha 2}, b_{\alpha 3}, \ldots\}$ で置き換え，新しい集合を $\widetilde{M}$ と呼ぶ．$\alpha < \beta$ のときは $b_{\alpha i} < b_{\beta j}$ で，$i < j$ の

とき $b_{\alpha i} < b_{\alpha j}$ と置けば，$\widetilde{M}$ もまた整列している．$\widetilde{\mu}$ を $\widetilde{M}$ の順序数とする．M は $\widetilde{M}$ の部分集合なので，以前の議論により，$\mu \leq \widetilde{\mu}$ である．$\mu = \widetilde{\mu}$ なら，M は $\widetilde{M}$ に相似であり，$\mu < \widetilde{\mu}$ なら，M は $\widetilde{M}$ のある切片に相似である．さて，M の順序付け $\omega_{\mathbf{m}}$ には最終元がないから（命題 5），どちらの場合でも，M は可算集合 B_β の和集合，それゆえ同じ濃度の集合の和集合に相似である．

あとは易しい．$\varphi : \bigcup B_\beta \longrightarrow M$ を全単射とし，$\varphi(B_\beta) = \{\alpha_1, \alpha_2, \alpha_3, \ldots\}$ であるとする．各 α_i を A_{α_i} で置き換え，和集合 $\bigcup A_{\alpha_i}$ を考える．$\bigcup A_{\alpha_i}$ は**可算個**の可算集合の和集合（それゆえ可算）だから，B_β は $\bigcup A_{\alpha_i}$ と同じサイズを持つ．言い換えれば，すべての β に対して，B_β から $\bigcup A_{\alpha_i}$ への全単射が，それゆえ，$\bigcup B_\beta$ から $\bigcup A_\alpha$ への全単射 ψ が存在する．しかしこのとき，$\psi\varphi^{-1}$ は M から $\bigcup A_\alpha$ への全単射になっており，こうして $|\bigcup A_\alpha| = \mathbf{m}$ が得られる．□

参考文献

[1] L. E. J. ブラウエル：「次元数の不変性の証明」(*Beweis der Invarianz der Dimensionszahl*), Math. Annalen **70** (1911), 161-165.

[2] P. エルデシュ：「連続体仮説に関連した補間問題」(*An interpolation problem associated with the continuum hypothesis*), Michigan Math. J. **11** (1964), 9-10.

[3] E. カムケ：『集合論』(*Theory of Sets*), Dover Books 1950.



「さらに無限個の濃度[2]」

[2] ［訳註］絵の下には，「最小の無限濃度　KH ホフマン 1998」という手書きの文字を読みとることができる．

第16章　不等式を賛えて

たとえば，ハーディー，リトルウッド，ポーヤの有名な著書『不等式』に見られるように，解析学には不等式が溢れている．基本的な不等式を2つ取り上げ，それぞれ2つの応用を述べ，天書の証明のチャンピオンの1人ジョルジュ・ポーヤが，最も適切な証明とはどんなものであると考えていたか，彼の言葉に耳を傾けることにしよう．

最初に扱う不等式の発見者は，コーシーとシュヴァルツ，それにと言うか，またはと言うかブニャコフスキーであると，色々な形で言われている．

定理 I（コーシー–シュヴァルツの不等式）
$\langle \boldsymbol{a}, \boldsymbol{b} \rangle$ を実ベクトル空間 V 上の内積とする（ノルムは $|\boldsymbol{a}|^2 = \langle \boldsymbol{a}, \boldsymbol{a} \rangle$）．そのとき，すべてのベクトル $\boldsymbol{a}, \boldsymbol{b} \in V$ に対して

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle^2 \quad \leq \quad |\boldsymbol{a}|^2 |\boldsymbol{b}|^2$$

が成り立つ．等号が成り立つのは，$\boldsymbol{a}$ と $\boldsymbol{b}$ が1次従属のとき，かつそのときに限る．

■ **証明.** 以下の（誰からともなく伝承された）証明がおそらく最短のものだろう．変数 x に関する2次関数

$$|x\boldsymbol{a} + \boldsymbol{b}|^2 \;=\; x^2 |\boldsymbol{a}|^2 + 2x \langle \boldsymbol{a}, \boldsymbol{b} \rangle + |\boldsymbol{b}|^2$$

を考える．$\boldsymbol{a} \neq \boldsymbol{0}$ としてよい．$\boldsymbol{b} = \lambda \boldsymbol{a}$ であれば明らかに $\langle \boldsymbol{a}, \boldsymbol{b} \rangle^2 = |\boldsymbol{a}|^2 |\boldsymbol{b}|^2$ となる．一方，$\boldsymbol{a}$ と $\boldsymbol{b}$ が1次独立なら，すべての x に対して $|x\boldsymbol{a} + \boldsymbol{b}|^2 > 0$ となるので，判別式 $\langle \boldsymbol{a}, \boldsymbol{b} \rangle^2 - |\boldsymbol{a}|^2 |\boldsymbol{b}|^2$ は 0 より小

さい. □

2 つ目の例は，調和平均，幾何（相乗）平均，算術（相加）平均の不等式である.

定理 II （調和，幾何，算術平均）
$a_1, \ldots, a_n$ を正の実数とすると,

$$\frac{n}{\frac{1}{a_1}+\cdots+\frac{1}{a_n}} \leq \sqrt[n]{a_1a_2\cdots a_n} \leq \frac{a_1+\cdots+a_n}{n}$$

が成り立つ．等号が成り立つのは，どちらの場合も，すべての a_i が等しいとき，かつそのときに限る.

■ **証明.** 以下の帰納法による証明は標準的ではないが美しく，コーシーによるものである（[7] 参照）. $P(n)$ を,

$$a_1a_2\cdots a_n \leq \left(\frac{a_1+\cdots+a_n}{n}\right)^n$$

の形に書いた第 2 の不等式の主張とする．$n = 2$ のときは，$a_1a_2 \leq (\frac{a_1+a_2}{2})^2 \Longleftrightarrow (a_1-a_2)^2 \geq 0$ だが，これは正しい．そこで，次の 2 つのステップに分けて行う.

(A) $P(n) \Longrightarrow P(n-1)$.

(B) $P(n)$ かつ $P(2) \Longrightarrow P(2n)$.

これらから明らかに，帰納法が成り立つ.

(A) の証明のためには，$A = \sum_{k=1}^{n-1} \frac{a_k}{n-1}$ とおく．すると,

$$\left(\prod_{k=1}^{n-1} a_k\right)A \overset{P(n)}{\leq} \left(\frac{\sum_{k=1}^{n-1} a_k + A}{n}\right)^n = \left(\frac{(n-1)A+A}{n}\right)^n = A^n$$

となって，$\prod_{k=1}^{n-1} a_k \leq A^{n-1} = \left(\frac{\sum_{k=1}^{n-1} a_k}{n-1}\right)^{n-1}$ が得られる.

(B) については,

$$\prod_{k=1}^{2n} a_k = \Big(\prod_{k=1}^{n} a_k\Big)\Big(\prod_{k=n+1}^{2n} a_k\Big) \overset{P(n)}{\le} \Big(\sum_{k=1}^{n}\frac{a_k}{n}\Big)^n\Big(\sum_{k=n+1}^{2n}\frac{a_k}{n}\Big)^n$$
$$\overset{P(2)}{\le} \left(\frac{\sum_{k=1}^{2n}\frac{a_k}{n}}{2}\right)^{2n} = \left(\frac{\sum_{k=1}^{2n} a_k}{2n}\right)^{2n}$$

となる[1]．等号に対する条件は容易に導かれる．調和平均と幾何平均との間の左の不等式は，ここで，$\frac{1}{a_1},\dots,\frac{1}{a_n}$ を考えればよい． □

■ **別証．** 算術・幾何平均不等式の数ある証明（モノグラフ [2] には 50 以上の証明が挙げられている）の中から，最近得られた，特に印象的なアルツァーの証明を挙げることにしよう．これは，実際には，より強い不等式の証明になっている．つまり，任意の正数 $a_1,\dots,a_n$，$p_1,\dots,p_n$（$\sum_{i=1}^n p_i = 1$）に対して

$$a_1^{p_1}a_2^{p_2}\cdots a_n^{p_n} \quad\le\quad p_1a_1 + p_2a_2 + \cdots + p_na_n$$

が成り立つ．左辺の式を G，右辺を A と書く．$a_1 \le \cdots \le a_n$ と仮定してよい．明らかに $a_1 \le G \le a_n$ なので[2]，$a_k \le G \le a_{k+1}$ を満たす k があることになる．これから

$$\sum_{i=1}^{k} p_i \int_{a_i}^{G} \Big(\frac{1}{t}-\frac{1}{G}\Big)\,dt \;+\; \sum_{i=k+1}^{n} p_i \int_{G}^{a_i} \Big(\frac{1}{G}-\frac{1}{t}\Big)\,dt \;\ge\; 0 \qquad (1)$$

がわかる．すべての被積分関数が ≥ 0 だからである．(1) を書き直すと

$$\sum_{i=1}^{n} p_i \int_{G}^{a_i} \frac{1}{G}\,dt \;\ge\; \sum_{i=1}^{n} p_i \int_{G}^{a_i} \frac{1}{t}\,dt$$

となり，この左辺は

$$\sum_{i=1}^{n} p_i\,\frac{a_i - G}{G} \;=\; \frac{A}{G} - 1$$

---

1 ［訳註］$P(2)$ は，$\Big(\sum_{k=1}^{n}\frac{a_k}{n}\Big)^n\Big(\sum_{k=n+1}^{2n}\frac{a_k}{n}\Big)^n$ をいったん $\Big(\Big(\sum_{k=1}^{n}\frac{a_k}{n}\Big)\Big(\sum_{k=n+1}^{2n}\frac{a_k}{n}\Big)\Big)^n$ としてから，括弧の中に使う．

2 ［訳註］明らかに，$G = a_1^{p_1}a_2^{p_2}\cdots a_n^{p_n} \le a_n^{p_1+p_2+\cdots+p_n} = a_n$ である．$a_1 \le G$ も同様．

であり，右辺は

$$\sum_{i=1}^{n} p_i(\log a_i - \log G) = \log \prod_{i=1}^{n} a_i^{p_i} - \log G = 0$$

である．これから $\frac{A}{G} - 1 \geq 0$ が，つまり $A \geq G$ が得られる．等号の場合は，(1) のすべての被積分関数が 0 でないといけないが，それは $a_1 = \cdots = a_n = G$ ということである．　□

最初の応用例としては，多項式の根の位置に関するラゲールの美しい結果がある（[7] を参照）．

定理 1．多項式 $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ のすべての根が実数であると仮定する．そのとき，根は

$$-\frac{a_{n-1}}{n} \pm \frac{n-1}{n}\sqrt{a_{n-1}^2 - \frac{2n}{n-1}a_{n-2}}$$

を端点とする区間に含まれる．

■ **証明．** 根の 1 つを y とし，残りを $y_1, \ldots, y_{n-1}$ とすると，多項式は $(x-y)(x-y_1)\cdots(x-y_{n-1})$ となる．それから，

$$-a_{n-1} = y + y_1 + \cdots + y_{n-1},$$
$$a_{n-2} = y(y_1 + \cdots + y_{n-1}) + \sum_{i<j} y_i y_j$$

が得られ，よって

$$a_{n-1}^2 - 2a_{n-2} - y^2 \ = \ \sum_{i=1}^{n-1} y_i^2$$

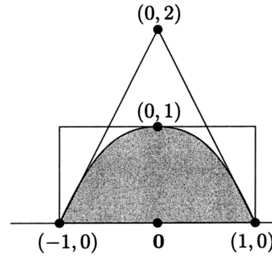
となる．コーシーの不等式を $(y_1, \ldots, y_{n-1})$ と $(1, \ldots, 1)$ に適用すれば，

$$(a_{n-1} + y)^2 = (y_1 + y_2 + \cdots + y_{n-1})^2$$
$$\leq (n-1)\sum_{i=1}^{n-1} y_i^2 \ = \ (n-1)(a_{n-1}^2 - 2a_{n-2} - y^2)$$

つまり，

$$y^2 + \frac{2a_{n-1}}{n}y + \frac{2(n-1)}{n}a_{n-2} - \frac{n-2}{n}a_{n-1}^2 \leq 0$$

が得られる．こうして，y は（それゆえすべての y_i は）この 2 次関数の 2 根の間にあり，この根が問題の区間の端点になっている． □



第 2 の応用例については，よく知られている放物線の初等的な性質から始める．放物線 $f(x) = 1 - x^2$ を，$x = -1$ と $x = 1$ の間で考える．$f(x)$ に対して，図にあるような**接線三角形**と**接線長方形**を考えよう．

影の領域の面積 $A = \int_{-1}^{1}(1 - x^2)dx$ が $\frac{4}{3}$ になり，三角形の面積 T と長方形の面積 R はともに 2 になることがわかる．こうして，$\frac{T}{A} = \frac{3}{2}$，$\frac{R}{A} = \frac{3}{2}$ となっている．

ポール・エルデシュとティボー・ガライは，美しい論文を書き，$f(x)$ が任意次数 n の実の多項式で，$-1 < x < 1$ に対して $f(x) > 0$ であり，$f(-1) = f(1) = 0$ を満たすとき，どんなことが起こるかを問題にした．そのとき面積 A は $\int_{-1}^{1} f(x)\, dx$ である．$f(x)$ がその最大値を，$(-1, 1)$ の中の b でとると仮定し，$R = 2f(b)$ とおく．-1 と 1 での接線を計算すると，すぐに

$$T \;=\; \frac{2f'(1)f'(-1)}{f'(1) - f'(-1)} \tag{2}$$

であり，また $f'(1) = f'(-1) = 0$ のときは $T = 0$ であることがわかる（次ページの箱を参照）．

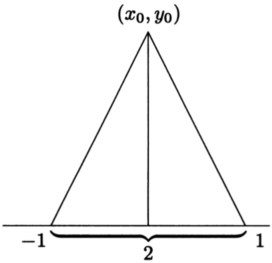
一般には，$\frac{T}{A}$ と $\frac{R}{A}$ に対する自明でない限界はない．これを見るには，$f(x) = 1 - x^{2n}$ とおく．すると，$T = 2n$, $A = \frac{4n}{2n+1}$ となって，$\frac{T}{A} > n$ となる．同様に，$R = 2$ なので，$\frac{R}{A} = \frac{2n+1}{2n}$ となり，n が無限に大きくなれば，1 に近づく．

しかし，エルデシュとガライが示したように，実根しか持たない多項式に対してはそのような限界が実際に存在するのである．

定理 2. $f(x)$ **を実根しか持たない** $n \geq 2$ **次の実多項式で，**$-1 < x < 1$ **に対しては** $f(x) > 0$ **であり，**$f(-1) = f(1) = 0$ **を満たすとする．そのとき，**

$$\frac{2}{3}T \;\leq\; A \;\leq\; \frac{2}{3}R$$

が成り立つ．等号の成立は，どちらの場合も，$n = 2$ **のときのみである．**



接線三角形

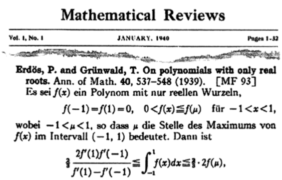
接線三角形の面積 T はまさに，2 本の接線の交点 (x_0, y_0) の座標 y_0 である．接線の方程式は $y = f'(-1)(x+1)$ と $y = f'(1)(x-1)$ なので，

$$x_0 = \frac{f'(1) + f'(-1)}{f'(1) - f'(-1)}$$

が得られ，

$$y_0 = f'(1)\left(\frac{f'(1) + f'(-1)}{f'(1) - f'(-1)} - 1\right) = 2\frac{f'(1)f'(-1)}{f'(1) - f'(-1)}$$

となる．


Mathematical Reviews

Vol. 1, No. 1　JANUARY, 1940　Pages 1–32

Erdös, P. and Grünwald, T. On polynomials with only real roots. Ann. of Math. **40**, 537–548 (1939). [MF 93]

Es sei $f(x)$ ein Polynom mit nur reellen Wurzeln,

$$f(-1) = f(1) = 0, \quad 0 < f(x) \leqq f(\mu) \quad \text{für } -1 < x < 1,$$

wobei $-1 < \mu < 1$, so dass μ die Stelle des Maximums von $f(x)$ im Intervall $(-1, 1)$ bedeutet. Dann ist

$$\frac{2}{3}\frac{2f'(1)f'(-1)}{f'(1) - f'(-1)} \leqq \int_{-1}^{1} f(x)dx \leqq \frac{2}{3} \cdot 2f(\mu),$$

エルデシュとガライは，入り組んだ帰納法を使ってこの結果を証明した．1940 年に数学評論 (Mathematical Reviews) 誌の第 1 号が出，その第 1 巻の第 1 ページにこの論文の評論が載った．ジョルジュ・ポーヤはそこで，左側の不等式が算術・幾何平均の不等式によっても証明できることを説明した．その証明は良心的な評論の美しい例であると同時に，天書の証明の美しい例でもある．

■ **$\frac{2}{3}T \leq A$ の証明．** $f(x)$ は実根しか持たず，そのどれも開区間 $(-1, 1)$ にはないのだから，最後には打ち消し合う正定数を忘れると，$\alpha_i \geq 1$，$\beta_j \geq 1$ として，

$$f(x) = (1 - x^2)\prod_i(\alpha_i - x)\prod_j(\beta_j + x) \tag{3}$$

の形に書くことができる．それゆえ，

$$A = \int_{-1}^{1}(1 - x^2)\prod_i(\alpha_i - x)\prod_j(\beta_j + x)dx$$

となる．$x \longmapsto -x$ という代入で，

$$A = \int_{-1}^{1}(1 - x^2)\prod_i(\alpha_i + x)\prod_j(\beta_j - x)dx$$

ともなり，だから，算術・幾何平均の不等式によって（すべての因子が ≥ 0 であることに注意），

$$\begin{aligned} A &= \int_{-1}^{1} \frac{1}{2}\Big[\ (1-x^2)\prod_i(\alpha_i - x)\prod_j(\beta_j + x) \ + \\ &\qquad (1-x^2)\prod_i(\alpha_i + x)\prod_j(\beta_j - x) \ \Big]dx \\ &\geq \int_{-1}^{1}(1-x^2)\Big(\prod_i(\alpha_i^2 - x^2)\prod_j(\beta_j^2 - x^2)\Big)^{1/2}dx \\ &\geq \int_{-1}^{1}(1-x^2)\Big(\prod_i(\alpha_i^2 - 1)\prod_j(\beta_j^2 - 1)\Big)^{1/2}dx \\ &= \frac{4}{3}\Big(\prod_i(\alpha_i^2 - 1)\prod_j(\beta_j^2 - 1)\Big)^{1/2} \end{aligned}$$

が得られる．$f'(1)$ と $f'(-1)$ を計算しよう．($f'(-1), f'(1) \neq 0$ と仮定してよい．さもなければ，$T = 0$ となって，不等式 $\frac{2}{3}T \leq A$ は自明になるからである．) (3) から

$$f'(1) \ = \ -2\prod_i(\alpha_i - 1)\prod_j(\beta_j + 1)$$

であることが，また同様に

$$f'(-1) \ = \ 2\prod_i(\alpha_i + 1)\prod_j(\beta_j - 1)$$

であることがわかる．それゆえ，結論として

$$A \ \geq \ \frac{2}{3}(-f'(1)f'(-1))^{1/2}$$

がわかる．

そこで，$-f'(1)$ と $f'(1)$ に，調和・幾何平均の不等式を使えば，(2) により

$$A \ \geq \ \frac{2}{3}\frac{2}{\frac{1}{-f'(1)} + \frac{1}{f'(-1)}} \ = \ \frac{4}{3}\frac{f'(1)f'(-1)}{f'(1) - f'(-1)} \ = \ \frac{2}{3}T$$

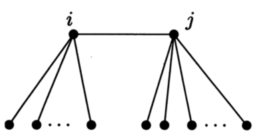
という結論が得られる．これが示したかったことである．出てきたすべての不等式での等号成立の条件を調べれば，容易に定理の最後の主張を示すことができる．□

定理2の第2の不等式の，同じように見事な証明を探すことは読者に残しておく．

さて，解析学はつまるところ不等式なのだが，グラフ理論からの例を1つ述べよう．そこではまったく予期せぬ形で不等式が使われている．第29章でトゥラーンの定理を議論するが，そのもっとも簡単な形が次の定理である．

定理 3. G を n 個の頂点上のグラフで，三角形を含まないとする．そのとき，G は高々 $\frac{n^2}{4}$ の辺を持つ．等号が成り立つのは，n が偶数で，G が完全2部グラフ $K_{n/2,n/2}$ のときだけである．

■ **第1の証明.** コーシーの不等式を用いたこの証明はマンテルによる．$V=\{1,\ldots,n\}$ を頂点集合とし，E を G の辺の集合とする．i の次数を d_i と書けば，$\sum_{i\in V} d_i = 2|E|$ である（2重に数えることに関する章の193ページ参照）．ij が辺であるとする．G には三角形がないのだから，$d_i + d_j \le n$ となる．というのは，i と j の両方に隣り合う頂点がないからである．



これから

$$\sum_{ij\in E}(d_i + d_j) \;\le\; n|E|$$

が得られる．和の中で，d_i はちょうど d_i 回だけ現れるので，

$$n|E| \;\ge\; \sum_{ij\in E}(d_i + d_j) \;=\; \sum_{i\in V} d_i^2$$

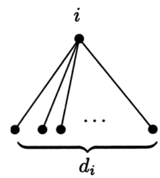
となり，コーシーの不等式を，ベクトル $(d_1,\ldots,d_n)^T$ と $(1,\ldots,1)^T$ に適用すると，

$$n|E| \;\ge\; \sum_{i\in V} d_i^2 \;\ge\; \frac{(\sum d_i)^2}{n} \;=\; \frac{4|E|^2}{n}$$

となり，結論が得られる．等号成立の場合には，すべての i,j に対して $d_i = d_j$ となり，さらに $d_i = \frac{n}{2}$ となる（$d_i + d_j = n$ だから）．G には

三角形がないので，このことから直ちに，$G = K_{n/2,n/2}$ であることがわかる． □

■ **第2の証明.** 算術・幾何平均の不等式を使った，定理3の以下の証明は，伝承された天書の証明である．α を最大の独立集合 A のサイズとし，$\beta = n - \alpha$ とおく．G には三角形がないので，頂点 i に隣り合う頂点の集合は独立な集合になり，すべての i に対して $d_i \leq \alpha$ となる．



サイズ β の集合 $B = V \backslash A$ は G のあらゆる辺の端点を含んでいる．G の辺を，B での端点に従って数えると，$|E| \leq \sum_{i \in B} d_i$ が得られる．すると，算術・幾何平均の不等式から，

$$|E| \;\leq\; \sum_{i \in B} d_i \;\leq\; \alpha\beta \;\leq\; \left(\frac{\alpha+\beta}{2}\right)^2 \;=\; \frac{n^2}{4}$$

が得られ，等号の場合はまた容易に扱うことができる[3]． □

参考文献

[1] H. アルツァー：「算術平均・幾何平均不等式の証明」(*A proof of the arithmetic mean-geometric mean inequality*), Amer. Math. Monthly **103** (1996), 585.

[2] P. S. ビュレン，D. S. ミトリノヴィッチ，P. M. ヴァシッチ：『平均とその不等式』(*Means and their Inequalities*), Reidel, Dordrecht 1988.

[3] P. エルデシュ，T. グリュンワルド：「実根しか持たない多項式について」(*On polynomials with only real roots*), Annals Math. **40** (1939), 537-548.

[4] G. H. ハーディー，J. E. リトルウッド，G. ポーヤ：『不等式』(*Inequalities*), Cambridge University Press, Cambridge 1952.

[5] W. マンテル：「問題 28」(*Problem 28*), Wiskundige Opgaven **10** (1906), 60-61.

[6] G. ポーヤ：「[3] の評論」(*Review of* [3]), Mathematical Reviews **1** (1940), 1.

[3] ［訳註］第3の等号条件から $\alpha = \beta$ が，第2の等号から $\alpha = d_i$（任意の i）が，第1の等号から $|E| = \alpha^2$ が得られる．

[7] G. ポーヤ, G. セゲー：『解析学における問題と定理　第I巻』(*Problems and Theorems in Analysis, Vol. I*), Springer-Verlag, Berlin Heidelberg New York 1972/78; Reprint 1998.

第17章　多項式に関するポーヤの定理



ジョルジュ・ポーヤ

解析学へのポーヤの多くの貢献の中でも，次のものは，結果が驚異であることと証明が美しいこととから，いつもエルデシュのお気に入りであった．

$$f(z) \;=\; z^n + b_{n-1}z^{n-1} + \cdots + b_0$$

を，最高次の係数が 1 の，$n \geq 1$ 次複素多項式とする．$f(z)$ に集合

$$\mathcal{C} \;=\; \{z \in \mathbb{C} : |f(z)| \leq 2\}$$

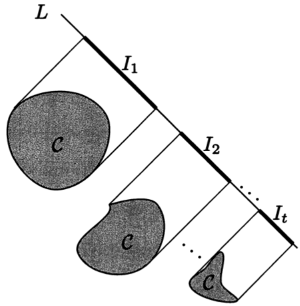
を対応させる．つまり，$\mathcal{C}$ は，f によって，複素平面の原点を中心とする半径 2 の円内に写される点の集合である．だから，$n = 1$ に対しては $\mathcal{C}$ は直径 4 の円盤に他ならない．

驚くほど簡単な議論で，ポーヤはこの集合 $\mathcal{C}$ の次のような美しい性質を明らかにしたのである．

> **複素平面に任意の直線 L をとり，集合 $\mathcal{C}$ から L への正射影 $\mathcal{C}_L$ を考える．そのとき，射影の全長は決して 4 を超えない**

$\mathcal{C}_L$ の全長が高々 4 とはどういう意味だろうか？ $\mathcal{C}_L$ が互いに交わらない区間 $I_1, \ldots, I_t$ の有限和であることがわかるので，条件は不等式 $\ell(I_1) + \cdots + \ell(I_t) \leq 4$ を意味することになる．ここで，$\ell(I_j)$ は通常の意味での区間の長さである．

平面を回転すれば，L が複素平面の実軸である場合を考えれば十分なことがわかる．これらのコメントを頭において，ポーヤの結果を述べる



ことにしよう.

定理 1. $f(z)$ **を少なくとも 1 次の複素多項式で，最高次の係数が 1 であるとする．** $\mathcal{C} = \{z \in \mathbb{C} : |f(z)| \leq 2\}$ **とおき，** $\mathcal{R}$ **を** $\mathcal{C}$ **の実軸への正射影とする．そのとき，実軸上の区間** $I_1, \ldots, I_t$ **であって，それらは** $\mathcal{R}$ **を被覆し，**

$$\ell(I_1) + \cdots + \ell(I_t) \ \leq \ 4$$

を満たすものが存在する．

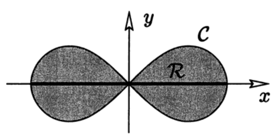
明らかに，定理の限界である 4 は $n = 1$ のときに達成されている．問題に対する感覚をもっとつかむために，これも限界の 4 を与える多項式 $f(z) = z^2 - 2$ を見てみよう．$z = x + iy$ が複素数なら，x は実軸への正射影である．それゆえ，

$$\mathcal{R} = \{x \in \mathbb{R} : x + iy \in \mathcal{C}\ (\text{ある } y \text{ に対して})\}$$

である．簡単な計算で，$f(z) = z^2 - 2$ に対して，$x + iy \in \mathcal{C}$ であることと

$$(x^2 + y^2)^2 \ \leq \ 4(x^2 - y^2)$$

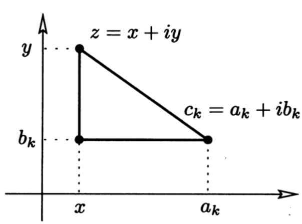
が同値であることが証明できる．これから $x^4 \leq (x^2 + y^2)^2 \leq 4x^2$ が得られ，$x^2 \leq 4$ となって，つまり，$|x| \leq 2$ がわかる．一方，$|x| \leq 2$ であるような $z = x \in \mathbb{R}$ は $|z^2 - 2| \leq 2$ を満たすので，$\mathcal{R}$ はちょうど長さ 4 の区間 $[-2, 2]$ であることがわかる．



$f(z) = z^2 - 2$

証明への第 1 段階として，$f(z) = (z - c_1) \cdots (z - c_n)$, $c_k = a_k + ib_k$ と書き，実多項式 $p(x) = (x - a_1) \cdots (x - a_n)$ を考える．$z = x + iy \in \mathcal{C}$ とすれば，ピュタゴラスの定理により，すべての k に対して

$$|x - a_k|^2 + |y - b_k|^2 = |z - c_k|^2$$



となるので，$|x - a_k| \leq |z - c_k|$ となり，つまり，

$$|p(x)| = |x - a_1| \cdots |x - a_n| \leq |z - c_1| \cdots |z - c_n| = |f(z)| \leq 2$$

となる．こうして，$\mathcal{R}$ が集合 $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \leq 2\}$ に含まれることがわかる．この集合 $\mathcal{P}$ が，高々 4 の全長を持つ区間によって被覆さ

れることを示すことができれば，お仕舞いである．したがって，主定理 1 は次の結果から得られることになる．

定理 2. $p(x)$ **は，次数** $n \geq 1$ **の実多項式で，最高次の係数が 1 で，すべての根が実数であるとする．そのとき，集合** $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \leq 2\}$ **は全長が高々 4 の区間で被覆される．**

ポーヤが論文 [2] で示したように，定理 2 は，今度は，以下に述べる有名なチェビシェフの結果から得られる．本章を自己充足なものにするために，附録で（ポーヤとセゲーの美しい解説に従った）証明を与えておく．

チェビシェフの定理.
$p(x)$ **を次数** $n \geq 1$ **で，最高次の係数が 1 の実多項式とする．そのとき**

$$\max_{-1 \leq x \leq 1} |p(x)| \;\geq\; \frac{1}{2^{n-1}}$$

が成り立つ．

まず，直ちにわかることを注意しておく．

系. $p(x)$ **を次数** $n \geq 1$ **で，最高次の係数が 1 の実多項式とし，区間** $[a, b]$ **のすべての** x **に対して** $|p(x)| \leq 2$ **であるとする．そのとき，**$b - a \leq 4$ **である．**

■ **証明.** $y = \frac{2}{b-a}(x-a) - 1$ という変換を考える．この写像は x の区間 $[a, b]$ を y の区間 $[-1, 1]$ の上に写す．対応する多項式

$$q(y) \;=\; p(\tfrac{b-a}{2}(y+1) + a)$$

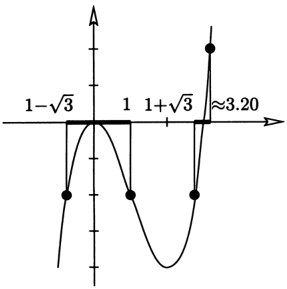
の最高次の係数は $(\frac{b-a}{2})^n$ となり，

$$\max_{-1 \leq y \leq 1} |q(y)| \;=\; \max_{a \leq x \leq b} |p(x)|$$

を満たす．チェビシェフの定理により，

$$2 \;\geq\; \max_{a \leq x \leq b} |p(x)| \;\geq\; (\tfrac{b-a}{2})^n \tfrac{1}{2^{n-1}} \;=\; 2(\tfrac{b-a}{4})^n$$

が得られ，こうして求めていた $b - a \leq 4$ が得られる． □



多項式 $p(x) = x^2(x-3)$ に対しては，$\mathcal{P} = [1-\sqrt{3}, 1] \cup [1+\sqrt{3}, \approx 3.2]$ となる．

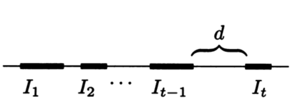
この系は，すでに定理 2 の主張に非常に近いものになっている．もし集合 $\mathcal{P} = \{x : |p(x)| \le 2\}$ が**区間**なら，$\mathcal{P}$ の長さは高々 4 である．しかし，集合 $\mathcal{P}$ は区間ではないかもしれない．余白に示した例では，$\mathcal{P}$ は 2 つの区間からなっている．

$\mathcal{P}$ について何が言えるのだろうか？ $p(x)$ は連続関数だから，ともかく $\mathcal{P}$ が交わらない閉区間 $I_1, I_2, \ldots$ の和であることと，区間 I_j の各端点での値が 2 か -2 であることはわかっている．このことから，有限個の区間 $I_1, \ldots, I_t$ しかないことがわかる．というのは，$p(x)$ はどんな値も有限回しか取り得ないからである．

ポーヤの素晴らしいアイデアは，最高次が 1 の別の n 次多項式 $\tilde{p}(x)$ で，$\widetilde{\mathcal{P}} = \{x : |\tilde{p}(x)| \le 2\}$ が**区間**であり，その長さが少なくとも $\ell(I_1) + \cdots + \ell(I_t)$ であるようなものを構成するということにある．それができれば，系から $\ell(I_1) + \cdots + \ell(I_t) \le \ell(\widetilde{\mathcal{P}}) \le 4$ が示され，証明が終わる．

■ **定理 2 の証明．** $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \le 2\} = I_1 \cup \cdots \cup I_t$ であるような $p(x) = (x-a_1)\cdots(x-a_n)$ を考え，区間 I_j を，I_1 が一番左で，I_t が一番右になるように並べる．まず，どの I_j も $p(x)$ の根を含んでいることを示そう．$p(x)$ が I_j の端点では 2 か -2 の値をとることはわかっている．もし 1 つの値が 2 でもう 1 つの値が -2 なら，確かに I_j の中に根がある．そこで，両方の端点で $p(x) = 2$ であると仮定する（-2 の場合は同じようにできる）．$b \in I_j$ を，I_j の中で $p(x)$ が最小値をとる点とする．すると，$p'(b) = 0$ かつ $p''(b) \ge 0$ となる．もし $p''(b) = 0$ なら，b は $p'(x)$ の重根であって，次にある箱の中の事実 1 によって $p(x)$ の根でもある．一方，$p''(b) > 0$ であれば，同じ箱の事実 2 から $p(b) \le 0$ であることがわかる．それゆえ，$p(b) = 0$ となってそれ自身が根であるか，$p(b) < 0$ となって b と I_j の端点との間に根が見つかる．

証明の最後のアイデアを述べよう．$I_1, \ldots, I_t$ を上の区間とし，一番右の区間 I_t が重複度も込めて $p(x)$ の m 個の根を含んでいるとする．$m = n$ なら（上で示したことから）I_t が唯一の区間となり，証明は終わっている．そこで $m < n$ と仮定し，図にあるように，d を I_{t-1} と I_t との間の距離とする．$b_1, \ldots, b_m$ を I_t の中にある $p(x)$ の根とし，$c_1, \ldots c_{n-m}$ を残りの根とする．そこで，$p(x)$ を分解して，$p(x) = q(x)r(x)$, $q(x) = (x-b_1)\cdots(x-b_m)$, $r(x) = (x-c_1)\cdots(x-c_{n-m})$ と書いて，$p_1(x) = q(x+d)r(x)$ とおく．$p_1(x)$ はまた n 次多項式で，最高次の係数も 1 である．$x \in I_1 \cup \cdots \cup I_{t-1}$ に対しては，すべての i



に対し $|x+d-b_i| < |x-b_i|$ となり，それゆえ $|q(x+d)| < |q(x)|$ である．これから

$$|p_1(x)| \leq |p(x)| \leq 2 \qquad (x \in I_1 \cup \cdots \cup I_{t-1})$$

となる．一方，$x \in I_t$ であれば，$|r(x-d)| \leq |r(x)|$ となるので，

$$|p_1(x-d)| = |q(x)||r(x-d)| \leq |p(x)| \leq 2$$

となって，結局 $I_t - d \subseteq \mathcal{P}_1 = \{x : |p_1(x)| \leq 2\}$ ということになる．

まとめると，$\mathcal{P}_1$ は $I_1 \cup \cdots \cup I_{t-1} \cup (I_t - d)$ を含むので，全長は $\mathcal{P}$ と同じだけはあることになる．ここで，$p(x)$ から $p_1(x)$ に変わると，区間 I_{t-1} と $I_t - d$ が合わさって 1 つの区間になっていることに注意しておく．$\mathcal{P}_1$ を構成する $p_1(x)$ の区間 $J_1, \ldots, J_s$ は少なくとも $\ell(I_1) + \cdots + \ell(I_t)$ の全長を持ち，一番右の区間 J_s に含まれる根の数は m より大きい．この手続きを高々 $t-1$ 回繰り返せば，最後に得られる多項式 $\tilde{p}(x)$ に対しては，$\widetilde{\mathcal{P}} = \{x : |\tilde{p}(x)| \leq 2\}$ は長さ $\ell(\widetilde{\mathcal{P}}) \geq \ell(I_1) + \cdots + \ell(I_t)$ の区間になり，証明が完結する． □

実根を持つ多項式に関する 2 つの事実

$p(x)$ を定数でない多項式で，根は実根のみとする．

事実 1. **b が $p'(x)$ の重根なら，b は $p(x)$ の根でもある．**

■ **証明.** $b_1, \ldots, b_r$ を $p(x)$ のそれぞれ重複度 $s_1, \ldots, s_r$ の根とする．$\sum_{j=1}^{r} s_j = n$ である．$p(x) = (x-b_j)^{s_j} h(x)$ であるから，$s_j \geq 2$ であれば，b_j は $p'(x)$ の根であり，b_j の $p'(x)$ での重複度は $s_j - 1$ となる．さらに，$p'(x)$ の根は，b_1 と b_2 の間にも，b_2 と b_3 の間にも，... ，b_{r-1} と b_r の間にも存在し，それらの根は**単根**である．というのも，$\sum_{j=1}^{r}(s_j - 1) + (r-1)$ を計算すると，すでに $p'(x)$ の次数である $n-1$ になってしまうからである．その結果，$p'(x)$ の**重根**は $p(x)$ の根以外には有り得ないことになる． □

事実 2. すべての $x \in \mathbb{R}$ に対して $p'(x)^2 \ge p(x)p''(x)$ である．

■ **証明．** x が $p(x)$ の根 $x = a_i$ なら示すべきことはないので，x は根ではないと仮定する．積の微分の公式から，

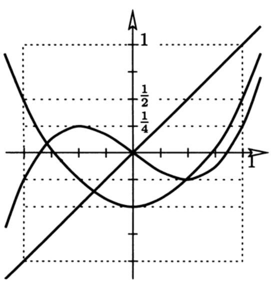
$$p'(x) = \sum_{k=1}^{n} \frac{p(x)}{x - a_k},$$
$$p''(x) = \sum_{k=1}^{n} \sum_{\substack{\ell=1 \\ \ell \ne k}}^{n} \frac{p(x)}{(x-a_k)(x-a_\ell)} = 2p(x) \sum_{\{k,\ell\}} \frac{1}{(x-a_k)(x-a_\ell)}$$

が得られる．ここで，$\{k,\ell\}$ はすべての対 $\{k,\ell\} \subseteq \{1,\dots,n\}$ を動く．それゆえ，

$$p'(x)^2 = p(x)^2 \Big(\sum_{k=1}^{n} \frac{1}{x-a_k} \Big)^2$$
$$> 2p(x)^2 \sum_{\{k,\ell\}} \frac{1}{(x-a_k)(x-a_\ell)} \quad = \quad p(x)p''(x)$$

となる．□

附録：チェビシェフの定理



多項式 $p_1(x) = x$, $p_2(x) = x^2 - \frac{1}{2}$, $p_3(x) = x^3 - \frac{3}{4}x$ はチェビシェフの定理の等号を満たす．

定理． $p(x)$ を，$n \ge 1$ 次の実多項式で，n 次の係数が **1** であるものとする．そのとき

$$\max_{-1 \le x \le 1} |p(x)| \ \ge \ \frac{1}{2^{n-1}}$$

が成り立つ．

証明を始める前に，等号が成り立つ例を見てみよう．余白に描いたものは，1, 2, 3 次の多項式で，それぞれの場合に等号が成り立つもののグラフである．実際，あらゆる次数で，チェビシェフの定理の等式が成り立つ多項式がちょうど 1 つずつ存在することがわかる[1]．

1 ［訳註］そのような多項式をチェビシェフの多項式と言う．

■ **証明．** 最高次の係数が 1 の実多項式 $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ を考える．領域 $-1 \le x \le 1$ の中だけに興味があるので，$x = \cos\vartheta$ とおき，得られる $\cos\vartheta$ の多項式を $g(\vartheta) = p(\cos\vartheta)$ と書くと，

$$g(\vartheta) = (\cos\vartheta)^n + a_{n-1}(\cos\vartheta)^{n-1} + \cdots + a_0 \tag{1}$$

となる．すると証明は以下の 3 段階で行われる．各段階はすべてそれ自身古典的な結果であり，興味深いものである．

(A) $g(\vartheta)$ をいわゆる**コサイン多項式**，つまり，

$$g(\vartheta) \;=\; b_n \cos n\vartheta + b_{n-1}\cos(n-1)\vartheta + \cdots + b_1\cos\vartheta + b_0 \tag{2}$$

($b_k \in \mathbb{R}$) の形の多項式で表わし，その最高次の係数が $b_n = \frac{1}{2^{n-1}}$ であることを示す．

(B) 位数 n（λ_n が 0 でない最高次の係数であるという意味）のコサイン多項式

$$h(\vartheta) \;=\; \lambda_n \cos n\vartheta + \lambda_{n-1}\cos(n-1)\vartheta + \cdots + \lambda_0 \tag{3}$$

が与えられたとき，$|\lambda_n| \le \max|h(\vartheta)|$ であることを示す．これを $g(\vartheta)$ に適用すると定理の証明が得られる．

(C) (B) を証明する途中で，次の注目すべき結果を示す．もし $h(\vartheta) = \lambda_n \cos n\vartheta + \cdots + \lambda_0$ が位数 n の**非負**なコサイン多項式であれば，$|\lambda_n| \le \lambda_0$ である．

(A) の証明． (1) から (2) の表示に移るには，すべてのベキ $(\cos\vartheta)^k$ をコサイン多項式として表わす必要がある．たとえば，コサインに対する加法定理から

$$\cos 2\vartheta \;=\; \cos^2\vartheta - \sin^2\vartheta \;=\; 2\cos^2\vartheta - 1$$

となるので，$\cos^2\vartheta = \frac{1}{2}\cos 2\vartheta + \frac{1}{2}$ となる．任意のベキ $(\cos\vartheta)^k$ に対してこれをするために，関係式 $e^{ix} = \cos x + i\sin x$ を使って，複素数に移る．e^{ix} は絶対値 1 の複素数である（38 ページの 1 のベキ根についての箱を参照）．とくにこれから，

$$e^{in\vartheta} \;=\; \cos n\vartheta + i\sin n\vartheta \tag{4}$$

がわかる．一方，

$$e^{in\vartheta} = (e^{i\vartheta})^n = (\cos\vartheta + i\sin\vartheta)^n \tag{5}$$

だから，(4) と (5) の実部を等しいと置くと，$i^{4\ell+2} = -1$, $i^{4\ell} = 1$, $\sin^2\theta = 1 - \cos^2\theta$ から，

$$\begin{aligned}\cos n\vartheta &= \sum_{\ell\geq 0}\binom{n}{4\ell}(\cos\vartheta)^{n-4\ell}(1-\cos^2\vartheta)^{2\ell}\\ &\quad -\sum_{\ell\geq 0}\binom{n}{4\ell+2}(\cos\vartheta)^{n-4\ell-2}(1-\cos^2\vartheta)^{2\ell+1}\end{aligned} \tag{6}$$

が得られる．結果として $\cos n\vartheta$ が $\cos\vartheta$ の多項式で

$$\cos n\vartheta = c_n(\cos\vartheta)^n + c_{n-1}(\cos\vartheta)^{n-1} + \cdots + c_0 \tag{7}$$

となる．(6) から最高次の係数に対して

$$c_n = \sum_{\ell\geq 0}\binom{n}{4\ell} + \sum_{\ell\geq 0}\binom{n}{4\ell+2} = 2^{n-1}$$

が得られる．

ここで，議論の向きを反転させる．帰納法により，$k < n$ に対して，$(\cos\vartheta)^k$ が位数 k のコサイン多項式として表わすことができるとすると，(7) から，$(\cos\vartheta)^n$ は，最高次の係数が $b_n = \frac{1}{2^{n-1}}$ である位数 n のコサイン多項式として書くことができると推論される．

(C) の証明． $h(\vartheta)$ を (3) のような位数 n のコサイン多項式とする．$\cos(-\vartheta) = \cos\vartheta$ と $\sin(-\vartheta) = -\sin\vartheta$ により，(4) から

$$\cos k\vartheta = \frac{e^{ik\vartheta} + e^{-ik\vartheta}}{2}$$

がわかる．$z = e^{i\vartheta}$ とおけば，$h(\vartheta)$ を

$$\begin{aligned}h(\vartheta) &= \lambda_n\frac{z^n + z^{-n}}{2} + \cdots + \lambda_k\frac{z^k + z^{-k}}{2} + \cdots + \lambda_0\\ &= z^{-n}\left(\lambda_n\frac{z^{2n} + z^0}{2} + \cdots + \lambda_k\frac{z^{n+k} + z^{n-k}}{2} + \cdots + \lambda_0 z^n\right)\\ &= z^{-n}H(z)\end{aligned} \tag{8}$$

の形に書くことができる．$H(z)$ を変数を z とする複素関数として調べよう．$H(z)$ は $2n$ 次で，$\lambda_n \neq 0$ だから，$z=0$ で 0 にならない．さらに，

$$H(z) \quad = \quad z^{2n} H\Big(\frac{1}{z}\Big)$$

である．それゆえ，α が $H(z)$ の根なら $\frac{1}{\alpha}$ も根である．その上，$H(z)$ は実係数なので，共役複素数 $\overline{\alpha}$ やその逆数 $1/\overline{\alpha}$ も根である．$H(z)$ の $2n$ 個の根を次のように分類しよう．最初のグループには，$|\alpha|=1$ つまり $\alpha = 1/\overline{\alpha}$ を満たすすべての根 α を入れる．第 2 のグループには，$\alpha \neq 1/\overline{\alpha}$ であるもの，つまり α か $1/\overline{\alpha}$ の一方の絶対値が 1 より小さいものを入れる．だから，$H(z)$ を

$$H(z) = \frac{\lambda_n}{2} \prod_{|\alpha|=1} (z-\alpha) \prod_{0<|\beta|<1} (z-\beta)(z-\frac{1}{\overline{\beta}}) \tag{9}$$

の形に書くことができる．

ここで，すべての ϑ に対して $h(\vartheta) \geq 0$ であるという仮定を使うのである．$z = e^{i\vartheta}$ だから $|z|=1$ であり，したがって，

$$h(\vartheta) \quad = \quad |h(\vartheta)| \quad = \quad |H(z)|$$

である．$H(z)$ の根を (9) にあるように見てみよう．α が最初のグループの根で，$|\alpha|=1$ ならば，$h(\vartheta)$ の実根 $\widetilde{\vartheta}$, $0 \leq \widetilde{\vartheta} \leq 2\pi$ に対応して，$\alpha = e^{i\widetilde{\vartheta}}$ となる．等式 $h(\vartheta) = e^{-in\vartheta} H(e^{i\vartheta})$ を微分すると，$h(\vartheta)$ における根 $\widetilde{\vartheta}$ の重複度が，$H(z)$ の根としての $e^{i\widetilde{\vartheta}}$ の重複度と同じであることがすぐにわかる．しかし，$h(\vartheta)$ は非負だから，$\widetilde{\vartheta}$ は $h(\vartheta)$ の最小値を与えており，それゆえ重複度は**偶数**になることがわかる．第 2 のグループに移って，積 $|z-\beta||z-1/\overline{\beta}|$ を考える．$z\overline{z}=1$ だから，

$$\begin{aligned}|z-\frac{1}{\overline{\beta}}|^2 &= (z-\frac{1}{\overline{\beta}})(\overline{z}-\frac{1}{\beta}) = \frac{(z\overline{\beta}-1)(\overline{z}\beta-1)}{\beta\overline{\beta}} \\ &= \frac{\beta\overline{\beta}-z\overline{\beta}-\overline{z}\beta+1}{\beta\overline{\beta}} = \frac{(z-\beta)(\overline{z}-\overline{\beta})}{\beta\overline{\beta}} = \frac{|z-\beta|^2}{|\beta|^2}\end{aligned}$$

となり，だから

$$|z-\beta||z-\frac{1}{\overline{\beta}}| \quad = \quad \frac{|z-\beta|^2}{|\beta|}$$

となる．まとめると，ある $0 \neq c \in \mathbb{C}$ に対して，

$$h(\vartheta) = |H(z)| = |c| \prod_{|\alpha|=1} |z-\alpha|^2 \prod_{0<|\beta|<1} |z-\beta|^2$$

となり，次のリースの有名な定理が証明できたことになる（[3] 参照）：

> **$h(\vartheta)$ が位数 n の非負のコサイン多項式であれば，**
>
> $$h(\vartheta) = |u(z)|^2, \qquad z = e^{i\vartheta}$$
>
> **となる．ここで，$u(z) = u_n z^n + u_{n-1} z^{n-1} + \cdots + u_0$ は次数 n の多項式である．**

その上，$H(z)$ が実係数だから，$u(z)$ の根 α, β は共役の対になって出てくるので，$u(z)$ 自身も実係数 u_i を持つ多項式になる．つまり，$z = e^{i\vartheta}$，$\overline{z} = e^{-i\vartheta}$ なので，

$$\begin{aligned} h(\vartheta) &= (u_n z^n + \cdots + u_0)\,(u_n z^{-n} + \cdots + u_0) \\ &= z^{-n}(u_n z^n + \cdots + u_0)\,(u_n + \cdots + u_0 z^n) \end{aligned}$$

となる．これを表示 (8) と比べれば，

$$\begin{aligned} \lambda_0 &= u_0^2 + u_1^2 + \cdots + u_n^2, \\ \frac{\lambda_k}{2} &= u_n u_{n-k} + u_{n-1} u_{n-1-k} + \cdots + u_k u_0 \quad (0 < k \leq n) \end{aligned} \tag{10}$$

が得られ，とくに

$$\lambda_n = 2 u_n u_0 \tag{11}$$

となる．(10) と (11) を合わせると，

$$|\lambda_n| = 2|u_n||u_0| \leq u_0^2 + u_n^2 \leq u_0^2 + u_1^2 + \cdots + u_n^2 = \lambda_0 \tag{12}$$

が得られる．

(B) の証明． まず，定数項の係数が $\lambda_0 = 0$ である位数 $n \geq 1$ のコサイン多項式 $h(\vartheta) = \lambda_n \cos n\vartheta + \cdots + \lambda_1 \cos\vartheta$ を考える．$h(\vartheta)$ が正の値も負の値もとることを示そう．逆に，$h(\vartheta) \geq 0$ であると仮定する．すると (12) から，$|\lambda_n| \leq 0$ となり，つまり $\lambda_n = 0$ となって矛盾が出る．$h(\vartheta) \leq 0$ の場合も，$-h(\vartheta)$ に同じ議論をすればよい．

最後に (3) の形の一般のコサイン多項式 $h(\vartheta)$ に戻り，$M = \max h(\vartheta)$, $m = \min h(\vartheta)$ とおく．上に証明したことから，$M > \lambda_0 > m$ であることに注意する．非負のコサイン多項式 $M - h(\vartheta)$ と $h(\vartheta) - m$ を考えることにより，(12) によって，それぞれ

$$|\lambda_n| \leq M - \lambda_0 \quad \text{と} \quad |\lambda_n| \leq \lambda_0 - m \tag{13}$$

となることが結論され，つまり，

$$|\lambda_n| \;\leq\; \frac{M-m}{2} \;\leq\; \max(M, -m) \;=\; \max|h(\vartheta)| \tag{14}$$

が得られる．(B) の証明が終わり，チェビシェフの定理の証明も終わった．
□

(10)–(14) を使って，等式 $\max|g(\vartheta)| = \frac{1}{2^{n-1}}$ を満たす，最高次の係数が 1 である，位数 n のコサイン多項式は $g(\vartheta) = \frac{1}{2^{n-1}} \cos n\vartheta$ しかないことを示し[2]，この解析を完成させることは読者にも容易だろう．

多項式 $T_n(x) = \cos n\vartheta$, $x = \cos\vartheta$ は（第 1 種の）**チェビシェフの多項式**と呼ばれる．つまり，$\frac{1}{2^{n-1}} T_n(x)$ はチェビシェフの定理での等号を成り立たせる，n 次の係数が 1 の唯一の n 次多項式である．

参考文献

[1] P. L. チェビシェフ：『全集』(*Œuvres*), Vol. I, Acad. Imperiale des Sciences, St. Petersburg 1899, pp. 387-469.

[2] G. ポーヤ：「多重連結領域上の歪曲定理の一般化についての寄稿」(*Beitrag zur Verallgemeinerung des Verzerrungssatzes auf mehrfach zusammenhängenden Gebieten*), Sitzungsber. Preuss. Akad. Wiss. Berlin (1928), 228-232; Collected Papers Vol. I, MIT Press 1974, 347-351.

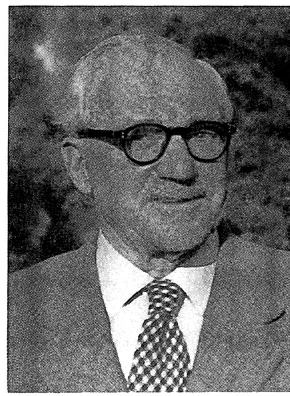
[3] G. ポーヤ，G. セゲー：『解析学における問題と定理　第 2 巻』(*Problems and Theorems in Analysis, Vol. II*), Springer-Verlag, Berlin Heidelberg New York 1976; Reprint 1998.

[2] ［訳註］とくに (12) が重要．

第18章　リトルウッドとオフォードの補題について

リトルウッドとオフォードは，代数方程式の根の分布について研究する中で，1943 年に次の結果を証明した．

> **$a_1, a_2, \dots, a_n$ を複素数で，すべての i に対して $|a_i| \geq 1$ であるとし，2^n 個の 1 次結合 $\sum_{i=1}^n \varepsilon_i a_i$，$\varepsilon_i \in \{1, -1\}$ を考える．そのとき，半径 1 のどんな円でも，その内部に入る和 $\sum_{i=1}^n \varepsilon_i a_i$ の数は，ある定数 $c > 0$ に対して**
>
> $$c \frac{2^n}{\sqrt{n}} \log n$$
>
> **を超えない．**



ジョン・E・リトルウッド

数年後ポール・エルデシュは，この限界を改良して $\log n$ の項を取り除いたが，さらに興味深いことに，これが実は，シュペルナーの定理（203 ページ参照）の単純な帰結であることを示した．

彼の議論に対する感じをつかむために，すべての a_i が実数である場合を見てみよう．($a_i < 0$ のときは，a_i を $-a_i$ に，ε_i を $-\varepsilon_i$ に変えることによって）すべての a_i が正であると仮定してよい．さて，1 次結合 $\sum \varepsilon_i a_i$ の集合が長さ 2 のある区間の内部にあるとしよう．$N = \{1, 2, \dots, n\}$ を添え字集合とする．あらゆる $\sum \varepsilon_i a_i$ に対して，$I = \{i \in N : \varepsilon_i = 1\}$ とおく．ここで，そのような 2 つの集合 $I \subsetneq I'$ に対しては

$$\sum \varepsilon_i' a_i - \sum \varepsilon_i a_i \;=\; 2 \sum_{i \in I' \setminus I} a_i \;\geq\; 2$$

シュペルナーの定理．
n 集合の部分列の反対鎖の大きさは高々 $\binom{n}{\lfloor n/2 \rfloor}$ である．

となるが，これは矛盾である．それゆえ集合 I は反対鎖[1]をなし，シュペルナーの定理から，そのような1次結合は高々 $\binom{n}{\lfloor n/2\rfloor}$ 個あるだけである．スターリングの定理（14ページ参照）により，ある $c>0$ に対して

$$\binom{n}{\lfloor n/2\rfloor} \;\le\; c\,\frac{2^n}{\sqrt{n}}$$

である．n が偶数で，すべて $a_i=1$ であれば，和が0になる $\binom{n}{n/2}$ 個の1次結合 $\sum_{i=1}^{n}\varepsilon_i a_i$ がある．区間 $(-1,1)$ を見れば，この2項係数が**厳密**な限界を与えていることがわかる．

同じ論文でエルデシュは以下の予想をしている．$\binom{n}{\lfloor n/2\rfloor}$ が複素数に対しても正しい限界であり（彼が証明できていたのは，ある c に対して $c\,2^n n^{-1/2}$ というだけだったが），実際には実ヒルベルト空間の $|\boldsymbol{a}_i|\ge 1$ を満たすベクトル $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_n$ に対しても，半径1の円を半径1の開球に置き換えれば，同じ限界が有効である，と予想した．

エルデシュは正しかったのだが，ギューラ・カトナとダニエル・クライトマンが，独立に複素数の場合に（または同じことだが平面 $\mathbb{R}^2$ に対して）証明をするまでには20年が掛かっている．彼らの証明は平面の2次元性をあからさまに使っていて，有限次元実ベクトル空間を含むように拡張するにはどうしたらよいか全く見えないものだった．

しかしその後1970年になって，クライトマンは驚くほど単純な議論で，ヒルベルト空間上の予想を完全な形で証明した．実際，彼はさらに多くのことを証明した．彼の議論は，正しい帰納法の仮定を見つけるときに実行可能な，素晴らしい例になっている．

ヒルベルト空間に馴染みのない読者に安心の言葉を．一般のヒルベルト空間の概念は実際には不必要である．有限個のベクトル $\boldsymbol{a}_i$ しか扱わないので，通常のスカラー積を持つ実空間 $\mathbb{R}^d$ を考えれば十分なのである．クライトマンの結果はこうである．

定理. $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_n$ **を** $\mathbb{R}^d$ **のベクトルで，長さが少なくとも1あるとし，**$R_1,\ldots,R_k$ **を** $\mathbb{R}^d$ **の** k **個の開領域で，同じ領域** R_i **に属するどんなに** $\boldsymbol{x},\boldsymbol{y}$ **対しても** $|\boldsymbol{x}-\boldsymbol{y}|<2$ **となっているとする．そのとき，領**

[1] ［訳註］反対鎖とは，どの2つの間にも鎖（この場合は包含関係）の関係がないことを意味する．この性質は，順序集合の部分集合に関するものである．

域の和集合 $\bigcup_i R_i$ に入り得る 1 次結合 $\sum_{i=1}^n \varepsilon_i \boldsymbol{a}_i$, $\varepsilon_i \in \{1,-1\}$ の数は，多くとも，大きい方から k 個の 2 項係数 $\binom{n}{j}$ の和になる．とくに，$k=1$ に対しては，$\binom{n}{\lfloor n/2 \rfloor}$ という限界を得る．

証明に移る前に，

$$\boldsymbol{a}_1 = \cdots = \boldsymbol{a}_n = \boldsymbol{a} = (1,0,\ldots,0)^T$$

に対してこれが厳密な限界になっていることに注意する．実際，偶数の n に対しては，$\binom{n}{n/2}$ 個の和は 0 になり，$\binom{n}{n/2-1}$ 個の和は $(-2)\boldsymbol{a}$ になり，$\binom{n}{n/2+1}$ 個の和は $2\boldsymbol{a}$ になり，などとなる．

$$-2\lceil \tfrac{k-1}{2} \rceil \boldsymbol{a}, \quad \ldots \quad , \quad (-2)\boldsymbol{a}, \quad \boldsymbol{0}, \quad 2\boldsymbol{a}, \quad \ldots \quad , \quad 2\lfloor \tfrac{k-1}{2} \rfloor \boldsymbol{a}$$

の周りに半径 1 の球を選ぶと，この k 個の球の中にある

$$\binom{n}{\lfloor \frac{n-k+1}{2} \rfloor} + \cdots + \binom{n}{\frac{n-2}{2}} + \binom{n}{\frac{n}{2}} + \binom{n}{\frac{n+2}{2}} + \cdots + \binom{n}{\lfloor \frac{n+k-1}{2} \rfloor}$$

個の和が得られ，これが約束した表示になる．というのは，2 項係数を大きい方からとれば，中心は真ん中あたりに来るからである（16 ページ参照）．n が奇数のときにも，同じような理屈が働く．

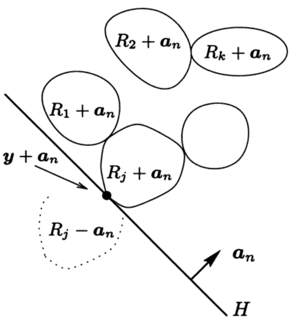
■ **証明.** 一般性を失うことなく，領域 R_i が互いに交わっていないと仮定してもよいので，以下では，そうすることにする．証明の鍵となるのは，2 項係数の漸化式で，それによって，n と $n-1$ の最大の 2 項係数がどう関係するかがわかる．$r = \lfloor \frac{n-k+1}{2} \rfloor, s = \lfloor \frac{n+k-1}{2} \rfloor$ とおくと，$\binom{n}{r}, \binom{n}{r+1}, \ldots, \binom{n}{s}$ が n に対する，大きい方から k 個の 2 項係数となる．漸化式 $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$ から

$$\begin{aligned}
\sum_{i=r}^{s} \binom{n}{i} &= \sum_{i=r}^{s} \binom{n-1}{i} + \sum_{i=r}^{s} \binom{n-1}{i-1} \\
&= \sum_{i=r}^{s} \binom{n-1}{i} + \sum_{i=r-1}^{s-1} \binom{n-1}{i} \qquad (1) \\
&= \sum_{i=r-1}^{s} \binom{n-1}{i} + \sum_{i=r}^{s-1} \binom{n-1}{i}
\end{aligned}$$

が得られ，簡単な計算によって，第 1 の和が大きい方から $k+1$ 個の 2 項係数 $\binom{n-1}{i}$ の和で，第 2 の和が大きい方から $k-1$ 個の和であることがわかる．

クライトマンの証明は n に関する帰納法で進められる．$n=1$ の場合は自明である．(1) があるので，帰納法の段階で示す必要があるのは，k 個の互いに交わらない領域にある $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_n$ の 1 次結合が，$k+1$ 個または $k-1$ 個の領域に属する $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{n-1}$ の 1 次結合の上に，全単射に写すことができることだけである．

主張．ずらした領域 $R_j-\boldsymbol{a}_n$ の少なくとも 1 つは，ずらした領域 $R_1+\boldsymbol{a}_n,\ldots,R_k+\boldsymbol{a}_n$ すべてと交わりを持たない．



これを証明するために，$\boldsymbol{a}_n$ に直交する超平面 $H=\{\boldsymbol{x}:\langle\boldsymbol{a}_n,\boldsymbol{x}\rangle=c\}$ であって，$\langle\boldsymbol{a}_n,\boldsymbol{x}\rangle\geq c$ で与えられる方の側にすべての $R_i+\boldsymbol{a}_n$ が含まれ，ある領域（たとえば $R_j+\boldsymbol{a}_n$ としよう）の閉包に接しているようなものを考える．すべての領域が有界なので，このような超平面は存在する．さて，R_j は開集合なので，任意の $\boldsymbol{x}\in R_j$ と R_j の閉包に属す任意の $\boldsymbol{y}$ に対して，$|\boldsymbol{x}-\boldsymbol{y}|<2$ となっている．$R_j-\boldsymbol{a}_n$ が H に関して反対側の中にあることを示したい．それとは反対に，ある $\boldsymbol{x}\in R_j$ に対して $\langle\boldsymbol{a}_n,\boldsymbol{x}-\boldsymbol{a}_n\rangle\geq c$，つまり $\langle\boldsymbol{a}_n,\boldsymbol{x}\rangle\geq|\boldsymbol{a}_n|^2+c$ であると仮定する．

点 $\boldsymbol{y}+\boldsymbol{a}_n$ で，H が $R_j+\boldsymbol{a}_n$ に接しているとすれば，$\boldsymbol{y}$ は R_j の閉包の点であり，$\langle\boldsymbol{a}_n,\boldsymbol{y}+\boldsymbol{a}_n\rangle=c$，つまり，$\langle\boldsymbol{a}_n,-\boldsymbol{y}\rangle=|\boldsymbol{a}_n|^2-c$ となる．それゆえ，

$$\langle\boldsymbol{a}_n,\boldsymbol{x}-\boldsymbol{y}\rangle \;\geq\; 2|\boldsymbol{a}_n|^2$$

となり，コーシー–シュヴァルツの不等式から，

$$2|\boldsymbol{a}_n|^2 \;\leq\; \langle\boldsymbol{a}_n,\boldsymbol{x}-\boldsymbol{y}\rangle \;\leq\; |\boldsymbol{a}_n||\boldsymbol{x}-\boldsymbol{y}|$$

と推論され，これから（$|\boldsymbol{a}_n|\geq 1$ だから）$2 \;\leq\; 2|\boldsymbol{a}_n| \;\leq\; |\boldsymbol{x}-\boldsymbol{y}|$ が得られるが，これは矛盾である．

残りは易しい．$R_1\cup\cdots\cup R_k$ に入る 1 次結合 $\sum\varepsilon_i\boldsymbol{a}_i$ を次のように分類する．1 組には，$\varepsilon_n=-1$ であるすべての $\sum_{i=1}^n\varepsilon_i\boldsymbol{a}_i$ と，$\varepsilon_n=1$ かつ R_j に属すすべての $\sum_{i=1}^n\varepsilon_i\boldsymbol{a}_i$ を入れ，2 組には，$\varepsilon_n=1$ かつ R_j に属さない残りの $\sum_{i=1}^n\varepsilon_i\boldsymbol{a}_i$ を入れる．すると，1 組に対応する 1 次結合 $\sum_{i=1}^{n-1}\varepsilon_i\boldsymbol{a}_i$ は，$k+1$ 個の互いに交わらない領域 $R_1+\boldsymbol{a}_n,\ldots,R_k+\boldsymbol{a}_n$,

$R_j - \boldsymbol{a}_n$ に入り，2 組に対応する 1 次結合 $\sum_{i=1}^{n-1} \varepsilon_i \boldsymbol{a}_i$ は $k-1$ 個の互いに交わらない $R_j - \boldsymbol{a}_n$ 以外の領域 $R_1 - \boldsymbol{a}_n, \ldots, R_k - \boldsymbol{a}_n$ に入る．帰納法により，1 組は高々 $\sum_{i=r-1}^{s} \binom{n-1}{i}$ 個の 1 次結合を含み，2 組は高々 $\sum_{i=r}^{s-1} \binom{n-1}{i}$ 個の 1 次結合を含む．そして (1) によりこれが，天書から直接に書き写された証明のすべてである． □

参考文献

[1] P. エルデシュ：「リトルウッドとオフォードの補題について」(*On a lemma of Littlewood and Offord*), Bulletin Amer. Math. Soc. **51** (1945), 898-902.

[2] G. カトナ：「エルデシュの予想とより強い形のシュペルナーの定理について」(*On a conjecture of Erdős and a stronger form of Sperner's theorem*), Studia Sci. Math. Hungar. **1** (1966), 59-63.

[3] D. クライトマン：「いくつかの和の分布に関するリトルウッドとオフォードの補題について」(*On a lemma of Littlewood and Offord on the distribution of certain sums*), Math. Zeitschrift **90** (1965), 251-259.

[4] D. クライトマン：「ベクトルの 1 次結合の分布に関するリトルウッドとオフォードの補題について」(*On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors*), Advances Math. **5** (1970), 155-157.

[5] J. E. リトルウッド，A. C. オフォード：「ランダムな代数方程式の実根の数について III」(*On the number of real roots of a random algebraic equation III*), Mat. USSR Sb. **12** (1943), 277-285.

第19章　コタンジェントとヘルグロッツのトリック

初等関数を含む一番興味深い公式は何だろうか？ ユルゲン・エルストロットはその美しい論文の中で，コタンジェント関数の部分分数展開

$$\pi \cot \pi x \;=\; \frac{1}{x} + \sum_{n=1}^{\infty} \left(\frac{1}{x+n} + \frac{1}{x-n} \right) \qquad (x \in \mathbb{R} \backslash \mathbb{Z})$$

をその第1の候補として挙げている．以下，彼の論文に従って述べて行く．

このエレガントな公式は，オイラーによって『無限解析入門』([3]) の §178 で証明されており，もちろん彼のもっとも素晴らしい業績の中に数えられている．この式はもっとエレガントに

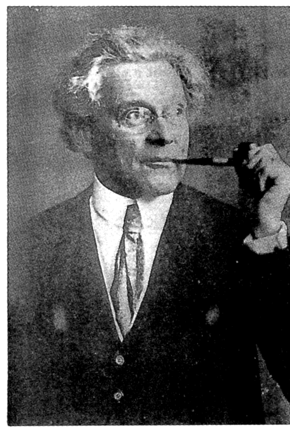
$$\pi \cot \pi x = \lim_{N \to \infty} \sum_{n=-N}^{N} \frac{1}{x+n} \tag{1}$$

と書くことができるが，和 $\sum_{n \in \mathbb{Z}} \frac{1}{x+n}$ の値を求めるというのは多少危険がある．というのも，この和は条件収束しかしないので，和の値は和をとる「正しい」順序によってしまうのである．

ギュスタヴ・ヘルグロッツに帰される驚くほど単純な議論 ——「ヘルグロッツのトリック」—— によって，(1) を導くことにする．始めるために，

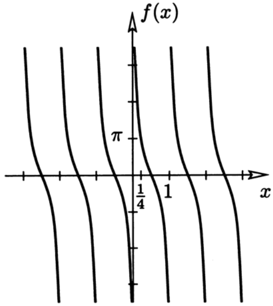
$$f(x) \;=\; \pi \cot \pi x, \qquad g(x) \;=\; \lim_{N \to \infty} \sum_{n=-N}^{N} \frac{1}{x+n}$$

とおき，最後にはこの2つの関数が一致してしまうことがわかるほどの，



ギュスタヴ・ヘルグロッツ

共通の関数の性質を導いてみることにしよう.



関数 $f(x) = \pi \cot \pi x$.

(A)　関数 $f(x)$ と $g(x)$ は整数以外のすべての値で定義され，そこで連続である.

コタンジェント関数 $f(x) = \pi \cot \pi x = \pi \frac{\cos \pi x}{\sin \pi x}$ に対して，このことは明らかである（図を見よ）. $g(x)$ については，恒等式 $\frac{1}{x+n} + \frac{1}{x-n} = -\frac{2x}{n^2-x^2}$ を使い，オイラーの公式を

$$\pi \cot \pi x = \frac{1}{x} - \sum_{n=1}^{\infty} \frac{2x}{n^2 - x^2} \tag{2}$$

と書き直す. (A) のためには，あらゆる $x \notin \mathbb{Z}$ に対して，級数

$$\sum_{n=1}^{\infty} \frac{1}{n^2 - x^2}$$

が x のある近傍で一様に収束することを証明しなければならない.

このためには，$n = 1$ の第1項や $2n - 1 \leq x^2$ を満たす項については，有限個しかないので問題は何もない. 一方，$n \geq 2$ かつ $2n - 1 > x^2$，つまり，$n^2 - x^2 > (n-1)^2 > 0$ を満たす項は，

$$0 \quad < \quad \frac{1}{n^2 - x^2} \quad < \quad \frac{1}{(n-1)^2}$$

によって上から抑えられており，このことは x 自身だけでなく，x のある近傍の値に対しても成り立っている. 最後に，$\sum \frac{1}{(n-1)^2}$ が収束する（さらに値が $\frac{\pi^2}{6}$ になることは44ページ参照）ことから，(A) の証明に必要な一様収束性が得られる.

(B)　f と g はともに周期1で**周期的**，つまり，すべての $x \in \mathbb{R} \backslash \mathbb{Z}$ に対して $f(x+1) = f(x)$ と $g(x+1) = g(x)$ が成り立つ.

コタンジェントは周期 π だから，f は周期1であることがわかる（もう一度上の図を参照）. g については次のようにする.

$$g_N(x) \; = \; \sum_{n=-N}^{N} \frac{1}{x+n}$$

とおくと，

$$g_N(x+1) = \sum_{n=-N}^{N} \frac{1}{x+1+n} \quad = \sum_{n=-N+1}^{N+1} \frac{1}{x+n}$$

$$= g_{N-1}(x) + \frac{1}{x+N} + \frac{1}{x+N+1}$$

となり，それゆえ，$g(x+1) = \lim_{N\to\infty} g_N(x+1) = \lim_{N\to\infty} g_{N-1}(x) = g(x)$ となる．

(C) f と g はともに奇関数，つまり，すべての $x \in \mathbb{R}\backslash\mathbb{Z}$ に対して，$f(-x) = -f(x)$ と $g(-x) = -g(x)$ が成り立つ．

関数 f は明らかにこの性質を持ち，g に対しては $g_N(-x) = -g_N(x)$ を見ればよい．

これからの，最後の 2 つの事実がヘルグロッツのトリックを構成する．つまり，最初に f と g が同じ関数等式を満たすことを示し，次に $h = f - g$ が $\mathbb{R}$ 全体に連続に拡張できることを示す．

(D) 2 つの関数 f と g は $f(\frac{x}{2})+f(\frac{x+1}{2}) = 2f(x)$ と $g(\frac{x}{2})+g(\frac{x+1}{2}) = 2g(x)$ という同じ関数等式を満たす．

$f(x)$ については，これはサインとコサインの加法定理の結果である．

$$f(\tfrac{x}{2}) + f(\tfrac{x+1}{2}) = \pi \left[\frac{\cos\frac{\pi x}{2}}{\sin\frac{\pi x}{2}} - \frac{\sin\frac{\pi x}{2}}{\cos\frac{\pi x}{2}} \right]$$

$$= 2\pi \frac{\cos(\frac{\pi x}{2} + \frac{\pi x}{2})}{\sin(\frac{\pi x}{2} + \frac{\pi x}{2})} \quad = \quad 2\,f(x).$$

加法定理．

$\sin(x+y) = \sin x \cos y + \cos x \sin y$

$\cos(x+y) = \cos x \cos y - \sin x \sin y$

$$\Longrightarrow \quad \sin(x+\tfrac{\pi}{2}) = \cos x$$
$$\cos(x+\tfrac{\pi}{2}) = -\sin x$$
$$\sin x = 2 \sin\tfrac{x}{2} \cos\tfrac{x}{2}$$
$$\cos x = \cos^2\tfrac{x}{2} - \sin^2\tfrac{x}{2}.$$

g についての関数等式は

$$g_N(\tfrac{x}{2}) \ + \ g_N(\tfrac{x+1}{2}) = 2\,g_{2N}(x) \ + \ \frac{2}{x+2N+1}$$

から得られ，これはまた

$$\frac{1}{\frac{x}{2}+n} + \frac{1}{\frac{x+1}{2}+n} = 2\Big(\frac{1}{x+2n} + \frac{1}{x+2n+1}\Big)$$

から得られる．

さて，

$$h(x) \;=\; f(x)-g(x) \;=\; \pi\cot\pi x-\Big(\frac{1}{x}-\sum_{n=1}^{\infty}\frac{2x}{n^2-x^2}\Big) \qquad (3)$$

を考えよう．これまでに，h が $\mathbb{R}\backslash\mathbb{Z}$ 上の連続関数で，性質 (B), (C), (D) を満たすことがわかっている．では，整数値では何が起こるのだろうか？ サインとコサインの級数展開から，もしくはド・ロピタルの定理を 2 回使うことによって，

$\cos x = 1-\frac{x^2}{2!}+\frac{x^4}{4!}-\frac{x^6}{6!}\pm\cdots$

$\sin x = x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}\pm\cdots$

$$\lim_{x\to 0}\Big(\cot x-\frac{1}{x}\Big) \;=\; \lim_{x\to 0}\frac{x\cos x-\sin x}{x\sin x} \;=\; 0$$

が得られ，それゆえまた

$$\lim_{x\to 0}\Big(\pi\cot\pi x-\frac{1}{x}\Big) \;=\; 0$$

が得られる．しかし，(3) の最後の和 $\sum_{n=1}^{\infty}\frac{2x}{n^2-x^2}$ は，$x\longrightarrow 0$ のとき 0 に収束するので，実際，$\lim_{x\to 0}h(x)=0$ となり，こうして周期性から，すべての $n\in\mathbb{Z}$ に対して

$$\lim_{x\to n}h(x) \;=\; 0$$

となる．

まとめると，次が示せたことになる．

(E)　$x\in\mathbb{Z}$ に対して $h(x)=0$ とおくと，h は $\mathbb{R}$ 全体の上の連続関数で，(B), (C), (D) に与えられた性質を満たしている．

止めの一撃に掛かる用意ができた．h は連続な周期関数だから，最大値 m を持つ．x_0 を $h(x_0)=m$ を満たす $[0,1]$ の点とする．(D) から

$$h(\tfrac{x_0}{2})+h(\tfrac{x_0+1}{2}) \;=\; 2m$$

が得られ，それゆえ，$h(\frac{x_0}{2})=m$ となる．これを繰り返せば，すべての n に対して $h(\frac{x_0}{2^n})=m$ となり，それゆえ，連続性から $h(0)=m$ となる．しかし，$h(0)=0$ だったから，$m=0$ である．つまり，すべての $x\in\mathbb{R}$ に対して，$h(x)\le 0$ である．$h(x)$ は奇関数なので，$h(x)<0$ となることはあり得ない．それゆえ，すべての $x\in\mathbb{R}$ に対して $h(x)=0$ となり，オイラーの定理は証明された．　□

(1) から非常に多くの系を導くことができる．中で一番有名なものは，リーマンのゼータ関数の正の偶数における値（第 6 章の附録参照）

$$\zeta(2k) \quad = \quad \sum_{n=1}^{\infty} \frac{1}{n^{2k}} \qquad (k \in \mathbb{N}) \tag{4}$$

に関するものである．

そこで，数年後の 1755 年に，オイラーが級数 (4) をどのように扱ったかを見て，話を終えることにしよう．公式 (2) から始める．(2) に x を掛けて，$y = \pi x$ と置けば，$|y| < \pi$ に対して

$$\begin{aligned} y \cot y &= 1 - 2 \sum_{n=1}^{\infty} \frac{y^2}{\pi^2 n^2 - y^2} \\ &= 1 - 2 \sum_{n=1}^{\infty} \frac{y^2}{\pi^2 n^2} \frac{1}{1 - \left(\frac{y}{\pi n}\right)^2} \end{aligned}$$

が得られる．最後の因子はある幾何数列の和になっているので，

$$\begin{aligned} y \cot y &= 1 - 2 \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \left(\frac{y}{\pi n}\right)^{2k} \\ &= 1 - 2 \sum_{k=1}^{\infty} \left(\frac{1}{\pi^{2k}} \sum_{n=1}^{\infty} \frac{1}{n^{2k}}\right) y^{2k} \end{aligned}$$

となり，次の注目すべき結果が得られたことになる．

すべての $k \in \mathbb{N}$ に対して，$y \cot y$ のベキ級数展開の y^{2k} の係数は

$$\left[y^{2k}\right] y \cot y \quad = \quad -\frac{2}{\pi^{2k}} \sum_{n=1}^{\infty} \frac{1}{n^{2k}} \quad = \quad -\frac{2}{\pi^{2k}} \zeta(2k) \tag{5}$$

に等しい．

$y \cot y$ のベキ級数展開を求めるには，おそらくずっと「標準的な」別の方法がある．解析学によって $e^{iy} = \cos y + i \sin y$ であることがわかっているので，

$$\cos y \quad = \quad \frac{e^{iy} + e^{-iy}}{2}, \qquad \sin y \quad = \quad \frac{e^{iy} - e^{-iy}}{2i}$$

であり，これから

$$y\cot y \;=\; iy\frac{e^{iy}+e^{-iy}}{e^{iy}-e^{-iy}} \;=\; iy\frac{e^{2iy}+1}{e^{2iy}-1}$$

が得られる．そこで $z=2iy$ を代入すると，

$$y\cot y \;=\; \frac{z}{2}\,\frac{e^z+1}{e^z-1} \;=\; \frac{z}{2}+\frac{z}{e^z-1} \tag{6}$$

となるので，必要なことは関数 $\frac{z}{e^z-1}$ のベキ級数展開だけである．これは $\mathbb{R}$ 全体の上で定義された連続関数であることに注意する（$z=0$ に対しては，指数関数のベキ級数展開を使うか，同じことだが，ド・ロピタルの定理を使えば，1 という値が得られる）．

$$\frac{z}{e^z-1} \;=\; \sum_{n\geq 0} B_n\frac{z^n}{n!} \tag{7}$$

と書くとき，係数 B_n は，**ベルヌーイ数**としてよく知られたものになる．(6) の左辺は**偶関数**（つまり，$f(z)=f(-z)$ を満たす）なので，奇数 $n\geq 3$ に対しては $B_n=0$ であり，一方，(6) の $\frac{z}{2}$ の項に対応して $B_1=-\frac{1}{2}$ であることがわかる．

$$\Big(\sum_{n\geq 0} B_n\frac{z^n}{n!}\Big)(e^z-1) \;=\; \Big(\sum_{n\geq 0} B_n\frac{z^n}{n!}\Big)\Big(\sum_{n\geq 1}\frac{z^n}{n!}\Big) \;=\; z$$

から，z^n の係数を比較すると，

$$\sum_{k=0}^{n-1}\frac{B_k}{k!(n-k)!} \;=\; \begin{cases} 1 & (n=1\text{ のとき}),\\ 0 & (n\neq 1\text{ のとき}) \end{cases} \tag{8}$$

n	0	1	2	3	4	5	6	7	8
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$

初めの方のベルヌーイ数

が得られる．(8) から，順にベルヌーイ数を計算していくことができる．$n=1$ の値で $B_0=1$ がわかり，$n=2$ からは $\frac{B_0}{2}+B_1=0$，つまり，$B_1=-\frac{1}{2}$ がわかり，などとなる．

もうほとんど終わりである．(6) と (7) を組み合わせると，

$$y\cot y \;=\; \sum_{k=0}^{\infty} B_{2k}\frac{(2iy)^{2k}}{(2k)!} \;=\; \sum_{k=0}^{\infty}\frac{(-1)^k 2^{2k}B_{2k}}{(2k)!}y^{2k}$$

となり，これに (5) を合わせると，$\zeta(2k)$ に対するオイラーの公式

$$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{(-1)^{k-1}2^{2k-1}B_{2k}}{(2k)!}\pi^{2k} \qquad (k \in \mathbb{N}) \qquad (9)$$

が得られる．そこでベルヌーイ数の表を見れば，第 6 章の和 $\sum \frac{1}{n^2} = \frac{\pi^2}{6}$ が得られるし，さらに

$$\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^6} = \frac{\pi^6}{945}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^8} = \frac{\pi^8}{9450},$$

$$\sum_{n=1}^{\infty} \frac{1}{n^{10}} = \frac{\pi^{10}}{93555}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^{12}} = \frac{691\,\pi^{12}}{638512875}, \quad \ldots$$

が得られる．

$\zeta(10)$ を与えてくれるベルヌーイ数 $B_{10} = \frac{5}{66}$ は無難な値に見えるが，$\zeta(12)$ に必要な次の値 $B_{12} = -\frac{691}{2730}$ には分子に大きな素数 691 が含まれている．オイラーは最初，ベルヌーイ数との関係に気づかずにいくつかの $\zeta(2k)$ の値を計算していたが，この奇妙な素数 691 に出くわして，初めて正しい道に気づいたのである．

ついでだが，$\zeta(2k)$ は $k \longrightarrow \infty$ のときに 1 に収束するので，等式 (9) から，数 $|B(2k)|$ が非常に速く大きくなることがわかる．これは最初の方の値からは明らかでないことである．

これに反して，奇数 $k \geq 3$ におけるリーマンのゼータ関数の値については，ほんの僅かなことしか知られていない（53 ページ参照）．

参考文献

[1] S. ボホナー：「ギュスタフ・ヘルグロッツの「全著作」の書評」(*Book review of "Gesammelte Schriften" by Gustav Herglotz*), Bulletin Amer. Math. Soc. **1** (1979), 1020-1022.

[2] J. エルストロット：「コタンジェントの部分分数展開，ヘルグロッツのトリック，ワイエルシュトラスの至るところ微分不可能な関数」(*Partialbruchzerlegung des Kotangens, Herglotz-Trick und die Weierstraßsche stetige, nirgends differenzierbare Funktion*), Math. Semesterberichte **45** (1998), 207-220.

[3] L. オイラー：『無限解析入門 I』(*Introductio in Analysin Infinitorum*), Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8. 英訳は *Introduction to Analysis of the Infinite*, Book I (translated by J.

D. Blanton), Springer-Verlag, New York 1988[1].

[4] L. オイラー：『微分法，およびその有限解析と級数論への応用』(*Institutiones calculi differentialis cum ejus usu in analysi finitorum ac doctrina serierum*), Petersburg 1755; Opera Omnia, Ser. 1, Vol. 10.

1 ［訳註］日本語訳は,『オイラーの無限解析』(高瀬正仁訳，海鳴社，2001).

第20章　ビュフォンの針の問題

フランス貴族，ジョルジュ・ルイ・レクレール，ビュフォン伯爵 (1707-1788) は，1777 年に次の問題を提出した．



ビュフォン伯爵

罫線入りの紙の上に短い針を落とすとする．そのとき，針がどれかの線と交わる確率はいくつか？

確率は，罫線の間の距離 d と落とす針の長さ ℓ による．というよりむしろ，その比 $\frac{\ell}{d}$ だけによる．目的からして，短い針というのは長さが $\ell \le d$ であるもののこととする．言い換えれば，短い針は同時に 2 本の線と交わることができ（ず，2 本の線に接することも確率 0 でしか起こら）ないものである．ビュフォンの問題の解答には驚かされるかも知れない．数 π が出てくるのである．

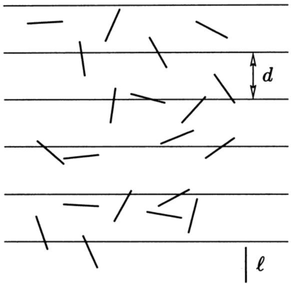
定理（「ビュフォンの針の問題」）

長さ ℓ の短い針が，同じ幅 $d \ge \ell$ で罫線の入った紙の上に落とされれば，針が罫線のどれかに交わる位置に来る確率は

$$p \quad = \quad \frac{2}{\pi}\frac{\ell}{d}$$

である．

この結果は，π の近似値を実験で求めることができることを意味している．針を N 回落として，P（回交わる）という正の答が得られれば，$\frac{P}{N}$ は近似的に $\frac{2}{\pi}\frac{\ell}{d}$ となる筈で，つまり，π は $\frac{2\ell N}{dP}$ で近似されるという



ことになる．もっとも大規模（で，徹底的）なテストはおそらく，1901 年にラザリニによって行われたものだろう．伝えられるところによると，彼は（$\frac{\ell}{d}=\frac{5}{6}$ の）棒を 3408 回落とすための機械を作ることまでした．そのとき，線と 1808 回交差したので，$\pi \approx 2\cdot\frac{5}{6}\frac{3408}{1808}=3.1415929\cdots$ という近似が得られたが，この値は 6 桁まで π と一致しており，この正しさは余りによすぎるものである．(ラザリニが選んだ値から直ちに，よく知られた近似値 $\pi\approx\frac{355}{113}$ が得られる[1]（44 ページ参照）．$\frac{5}{6}$3408 は 355 の倍数であり，3408 と $\frac{5}{6}$ を選んだことに，疑しさ以上のものがあることを示している．ラザリニの捏造（ねつぞう）についての議論は，[5] を参照のこと.）

針の問題はある積分の計算によっても解くことができる．あとでそれをして，さらにこの方法によって長い針に対する問題も解く．しかし，1860 年に E. バルビエによって示された天書の証明は積分を必要としない．別の針を落としたなら ....

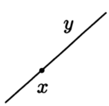
短いものであれ長いものであれ，どんな針を落としたとしても，交差の期待値は

$$E \;=\; p_1+2p_2+3p_3+\cdots$$

となる．ここで，p_1 は針が 1 本の線とだけ交差する確率で，p_2 は針が 2 本の線と交差する確率で，p_3 は 3 本のときの確率，などである．すると，ビュフォンが問題としている，少なくとも 1 本の針と交差する確率は

$$p \;=\; p_1+p_2+p_3+\cdots$$

となる.（針が 1 本の線に重なるとか，端点が線の 1 つの上に来るとかいう事象は確率 0 なので，ずっと無視して議論することができる.）



一方，針が短かければ，2 本以上の線との交差の確率は 0 で $p_2=p_3=\cdots=0$ だから，$E=p$ となる．つまり，求めたかった確率は，交差回数の期待値そのものとなる．このように定式化し直すのが究めて有効であるのは，期待値の線形性（112 ページ参照）を使うことができるようになるからである．実際，長さ ℓ の真っ直ぐな針を落とすことによって得られる交差数の期待値を $E(\ell)$ と書こう．もしこの長さが $\ell=x+y$ で，針を長さ x の「前部分」と長さ y の「後部分」に分けて考えれば，

---

[1] ［訳註］$2\frac{5}{6}\frac{3408}{1808}=5\frac{568}{904}=\frac{355}{113}$.

$$E(x+y) \;=\; E(x)+E(y)$$

が得られる．というのは，得られる交差は，つねに，前部分から得られるものと後部分から得られるものを足したものとして得られるからである．

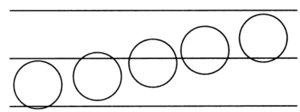
n に関する帰納法により，この「関数等式」から，すべての $n \in \mathbb{N}$ に対して $E(nx) = nE(x)$ であることが得られ，それから $mE(\frac{n}{m}x) = E(m\frac{n}{m}x) = E(nx) = nE(x)$ が得られるので，すべての**有理数** $r \in \mathbb{Q}$ に対して，$E(rx) = rE(x)$ が成り立つことになる．さらに，明らかに $E(x)$ は $x \geq 0$ に関して単調であり，これからすべての $x \geq 0$ に対して $E(x) = cx$ であることがわかる．ここで $c = E(1)$ はある定数である．

しかし，この定数はいくつなのだろうか？



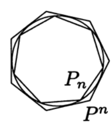
そのために，異なる形の針を使う．実際，全長が ℓ で，各部分が線分であるような「多角形的」な針を落としてみよう．そのときの交差回数は（確率 1 で）各部分での交差回数の和である．それゆえ，交差回数の期待値はまた，期待値の線形性から

$$E \;=\; c\ell$$



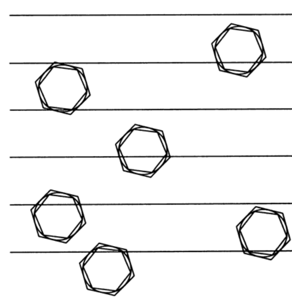
となる．(このためには，線分同士の繋ぎ目（ジョイント）が固定されているのか自由に動くかということは重要なことですらない！)

ビュフォンの針の問題のバルビエの解法の鍵は，直径 d の完全な円 C（長さは $x = d\pi$）であるような針を考えることである．そのような針を罫線入りの紙の上に落とせば，まさに 2 つの交点が常に得られる！



円は多角形で近似できる．円の針と一緒に，内接多角形 P_n と外接多角形 P^n を落としたと考えてみよう．P_n と交わる線はまた C と交わるし，線が C と交われば，P^n とも交わる．こうして，交差回数の期待値は

$$E(P_n) \;<\; E(C) \;<\; E(P^n)$$



を満たす．さて，P_n と P^n は多角形で，交差回数はともに，「長さの c 倍」と期待され，C に対しては 2 だったのだから，

$$c\ell(P_n) \;<\; 2 \;<\; c\ell(P^n) \qquad (1)$$

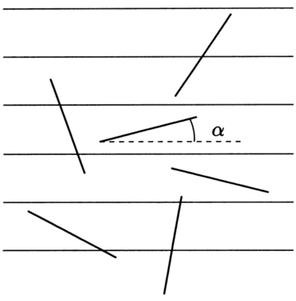
となる．P_n と P^n はともに，$n \longrightarrow \infty$ で C を近似する．とくに，

$$\lim_{n\to\infty} \ell(P_n) \;=\; d\pi \;=\; \lim_{n\to\infty} \ell(P^n)$$

となるが，$n \longrightarrow \infty$ のときは (1) から

$$c\,d\pi \quad \le \quad 2 \quad \le c\,d\pi$$

がわかり，これから $c = \frac{2}{\pi}\frac{1}{d}$ が得られる．　□



しかし，解析を使っても証明はできたのである！「簡単」な積分を得るためのトリックは，まず針の傾きを考えることである．落とした針が水平線と角 α をなすとしよう．ここで α の範囲は $0 \le \alpha \le \frac{\pi}{2}$ である．(傾きが負になる場合は無視する．というのは，この場合，正の傾きの場合と対称的で，同じ確率になるからである.）角 α で落ちている針の高さは $\ell \sin\alpha$ であり，そのような針が，間隔 d の水平線の 1 つと交わる確率は $\frac{\ell\sin\alpha}{d}$ である．だから，可能な角 α にわたって平均すれば，確率

$$p \;=\; \frac{2}{\pi}\int_0^{\pi/2} \frac{\ell\sin\alpha}{d}d\alpha \;=\; \frac{2}{\pi}\frac{\ell}{d}\Big[-\cos\alpha\Big]_0^{\pi/2} \;=\; \frac{2}{\pi}\frac{\ell}{d}$$

が得られる．

長い針に対して，まず $\ell\sin\alpha \le d$，つまり $0 \le \alpha \le \arcsin\frac{d}{\ell}$ の範囲では，同じ確率 $\frac{\ell\sin\alpha}{d}$ が得られる．しかしながら，より大きな角 α に対しては，針は必ず線と交わり，つまり，確率は 1 である．それゆえ，$\ell \ge d$ に対して，

$$\begin{aligned}
p &= \frac{2}{\pi}\Big(\int_0^{\arcsin(d/\ell)} \frac{\ell\sin\alpha}{d} + \int_{\arcsin(d/\ell)}^{\pi/2} 1\;dx\Big)\\
&= \frac{2}{\pi}\Big(\frac{\ell}{d}\Big[-\cos\alpha\Big]_0^{\arcsin(d/\ell)} + \Big(\frac{\pi}{2} - \arcsin\frac{d}{\ell}\Big)\Big)\\
&= 1 + \frac{2}{\pi}\Big(\frac{\ell}{d}\Big(1 - \sqrt{1-\frac{d^2}{\ell^2}}\Big) - \arcsin\frac{d}{l}\Big)
\end{aligned}$$

と計算される．

こんな風に，長い針に対する答は余りきれいなものではないが，これから面白い演習問題ができる．(安全のために)「p に対する式は $\ell = d$ のときは $\frac{2}{\pi}$ となり，ℓ に関して狭義単調増加で，$\ell \longrightarrow \infty$ のとき 1 に収束する」ことを示せ．

参考文献

[1] E. バルビエ：「針の問題と隠れたジョイントの働きに関するノート」(*Note sur le problème de l'aiguille et le jeu du joint couvert*), J. Mathématiques Pures et Appliquées (2) **5** (1860), 273-286.

[2] L. ベルグレン，J. ボウェイン，P. ボウェイン編：『π：原典』(*Pi: A Source Book*), Springer-Verlag, New York 1997.

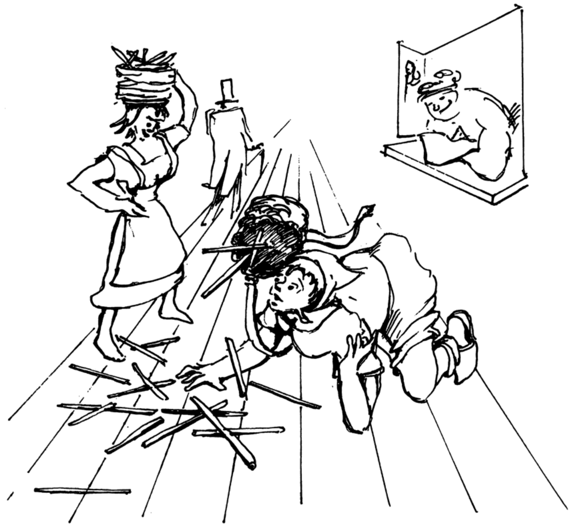
[3] G. L. レクレール，ビュフォン伯爵：「道徳的な算術試論」(*Essai d'arithmétique morale*),『一般および個別博物学』の附録 (Appendix to "Histoire naturelle générale et particulière"), Vol. 4, 1777.

[4] D. A. クレイン，G.-C. ロータ：『幾何学的確率論入門』(*Introduction to Geometric Probability*), "リンチェイ[2]講義 (Lezioni Lincee)," Cambridge University Press 1997.

[5] T. H. オバーン：『パズルとパラドクス』(*Puzzles and Paradoxes*), Oxford University Press, London 1965.

---

2 [訳註] リンチェイ・アカデミー (Academia dei Lincei) は，モンティチェリ候フェデリコ・チェージ (1585-1630) が 1603 年に創設した科学研究のための学会．リンチェとは山猫のことで，その目のように鋭く物事を見抜くという意味がある．ちなみに，ガリレオ・ガリレイは 5 番目の会員である．



「問題がわかったかい？」

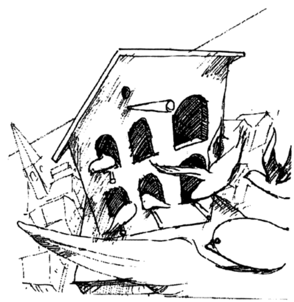
組合せ論



「メランコリーなラテン方陣」

第21章　鳩の巣と2重数え上げ

この章のタイトルの2つの原理のように，いくつかの数学の原理はあまりにも明白なので，同じように明白な結論しか生まないと考え勝ちなものである.「それがそうでもない」と納得して貰うために，ポール・エルデシュが天書の中に含めようと提案していた例を使って説明しよう．あとの方の章でもそういう例に出会うことになる.



「鳥の目から見た鳩の巣穴」

鳩の巣原理.
もし n 個のものが r 個の箱に入れられ，$r < n$ であれば，少なくとも1つの箱には2個以上のものが入っている.

まあ，これは確かに明らかで，証明しなければならないことはない．写像の言葉でこの原理を言い換えることができる.「N と R を2つの有限集合で，

$$|N| = n > r = |R|$$

であるとし，$f : N \longrightarrow R$ を写像とする．そのとき，ある $a \in R$ が存在して，$|f^{-1}(a)| \geq 2$ となる.」さらに強い不等式も得ることができる.「ある $a \in R$ が存在して，

$$|f^{-1}(a)| \;\geq\; \left\lceil \frac{n}{r} \right\rceil \tag{1}$$

となる.」実際，もしそうでなければ，すべての a に対して $|f^{-1}(a)| < \frac{n}{r}$ となり，$n = \sum_{a\in R} |f^{-1}(a)| < r\,\frac{n}{r} = n$ となるが，これはあり得ない.

1. 数

主張．数 $1, 2, 3, \ldots, 2n$ を考え，それから任意に $n+1$ 個をとる．この $n+1$ 個の数のうち，互いに素な 2 数が存在する．

これもまた明らかである．1 しか離れていない 2 数がなければならず，それらは互いに素である．

しかし，条件を反対にしてみよう．

主張．また $A \subseteq \{1, 2, \ldots, 2n\}$ かつ $|A| = n+1$ であるとする．そのとき，常に一方が他方を割る 2 数が A の中に存在する．

これはそんなに明らかなわけではない．エルデシュが話してくれたことがあるが，彼はこの問題を夕食の間にラホス・ポーサという若者に出したことがあり，食事が終わったときにラホスは答を得ていたという．これはずっと，エルデシュが好んで発する，数学への「入門」問題であった．（肯定的な）解答は鳩の巣原理によって与えられる．あらゆる数 $a \in A$ を $a = 2^k m$ という形に書く．ここで，m は 1 と $2n-1$ の間の奇数とする．A には $n+1$ 個の数があるが，異なる奇数は n 個しかないのだから，同じ奇数部分を持つ 2 数が A の中になければならない．そのとき一方は他方の倍数になる．□

$n+1$ を n に変えたらどちらの結果も正しくはない．このためにはそれぞれ，$\{2, 4, 6, \ldots, 2n\}$ と $\{n+1, n+2, \ldots, 2n\}$ という集合を考えればよい．

2. 数列

もう 1 つエルデシュのお気に入りの問題を挙げておく．この問題は，ラムゼイ問題についてのエルデシュとシェッカーズの論文に含まれている．

主張．$mn+1$ 個の異なる実数の作る任意の数列 $a_1, a_2, \ldots, a_{mn+1}$ の中には，長さ $m+1$ の増大部分列

$$a_{i_1} < a_{i_2} < \cdots < a_{i_{m+1}} \qquad (i_1 < i_2 < \cdots < i_{m+1})$$

か，長さ $n+1$ の減少部分列

$$a_{j_1} > a_{j_2} > \cdots > a_{j_{n+1}} \qquad (j_1 < j_2 < \cdots < j_{n+1})$$

のどちらかか，またはその双方が存在する．

この場合，鳩の巣原理の使い方は直接的ではない．各 a_i に対して，a_i から始まる**最長の増大**部分列の長さ t_i を対応させる．ある i に対して $t_i \geq m+1$ であれば，長さ $m+1$ の増大部分列があることになる．そこで，すべての i に対して $t_i \leq m$ と仮定する．関数 $f: a_i \longmapsto t_i$ は $\{a_1, \ldots, a_{mn+1}\}$ を $\{1, \ldots, m\}$ に写すが，(1) から，ある $s \in \{1, \ldots, m\}$ があって，$\frac{mn}{m}+1 = n+1$ 個の数 a_i に対して $f(a_i) = s$ となる．その数を $a_{j_1}, a_{j_2}, \ldots, a_{j_{n+1}}$ $(j_1 < \cdots < j_{n+1})$ とする．そこで連続した 2 数 $a_{j_i}, a_{j_{i+1}}$ を考える．もし $a_{j_i} < a_{j_{i+1}}$ なら，$a_{j_{i+1}}$ から始まる長さ s の増大部分列が得られ，その結果，a_{j_i} から始まる長さ $s+1$ の増大部分列が得られることになるが，$f(a_{j_i}) = s$ だからこれは起こり得ない．こうして，長さ $n+1$ の減少部分列 $a_{j_1} > a_{j_2} > \cdots > a_{j_{n+1}}$ が得られたことになる． □

mn 個の数に対してこの主張が一般には成り立たないことを示すのは，きっと面白いだろう．

単調部分列に関するこの単純に見える結果から，**グラフの次元**に関する高度に自明でない結論が得られる．ここでは，一般のグラフに対する次元の概念は必要でなく，ただ完全グラフ K_n に対してだけあればよい．それは，以下のように言うことができる．$N = \{1, \ldots, n\}$, $n \geq 3$ をとり，N の m 個の置換 $\pi_1, \ldots, \pi_m$ を考える．これらの置換 π_i が K_n の**表現**であるとは，あらゆる異なる 3 数 i, j, k に対して，k が i と j の両方のうしろにくるような置換 π が存在するときとする．そのとき，表現 $\pi_1, \ldots, \pi_m$ が存在する最小の m を K_n の次元とするのである．

たとえば $\dim(K_3) = 3$ である．というのは，$\pi_1 = (1,2,3)$, $\pi_2 = (2,3,1)$, $\pi_3 = (3,1,2)$ のように，3 数のうちの任意の数が最後に来ないといけないからである．では K_4 はどうだろうか？ まず，$\dim(K_n) \leq \dim(K_{n+1})$ に注意する．これには，K_{n+1} の表現から $n+1$ を取り去ればよい．だから，$\dim(K_4) \geq 3$ であり，実際，

$$\pi_1 = (1,2,3,4), \quad \pi_2 = (2,4,3,1), \quad \pi_3 = (1,4,3,2)$$

ととれば，$\dim(K_4) = 3$ がわかる．$\dim(K_5) = 4$ の証明もそんなに易しいわけではないが，そのあと，驚くことに，$n = 12$ まで次元は 4 のままで，$\dim(K_{13}) = 5$ となるのである．だから $\dim(K_n)$ はかなりワイルドな関数に見える．が，そんなことはない！ n を無限に大きくすると，$\dim(K_n)$ は実際，非常に行儀のよい関数になる．その下界を見つけ

π_1:	1	2	3	5	6	7	8	9	10	11	12	4
π_2:	2	3	4	8	7	6	5	12	11	10	9	1
π_3:	3	4	1	11	12	9	10	6	5	8	7	2
π_4:	4	1	2	10	9	12	11	7	8	5	6	3

この 4 つの置換は K_{12} の表現である．

る鍵は鳩の巣原理である．

$$\dim(K_n) \ \geq \ \log_2 \log_2 n \tag{2}$$

であることをを示そう．上で見たように $\dim(K_n)$ は n に関して単調な関数だから，$n = 2^{2^p} + 1$ に対して (2) を証明すれば十分である．つまり，

$$\dim(K_n) \ \geq \ p + 1 \qquad (n = 2^{2^p} + 1)$$

を示すことになる．そこで反対に，$\dim(K_n) \leq p$ であると仮定して，$\pi_1, \ldots, \pi_p$ を，$N = \{1, 2, \ldots, 2^{2^p} + 1\}$ を表現する置換とする．そこで，単調部分列に関する上の結果を p 回使う．π_1 の中に，長さが $2^{2^{p-1}} + 1$ の単調な部分列 A_1 が存在する（増大列か減少列かはどちらでもよい）．π_2 の中でこの集合 A_1 を見る．上の結果をもう一度使うと，長さが $2^{2^{p-2}} + 1$ の単調な部分列 A_2 が存在し，もちろん A_2 は π_1 の中でも単調である．これを続ければ，ついには**すべての**置換 π_i の中で単調な，長さが $2^{2^0} + 1 = 3$ である部分列 A_p が見つかる．$A_p = (a, b, c)$ とすると，**すべての** π_i の中で，$a < b < c$ か $a > b > c$ かになっている．しかし，b が a か c かのうしろにくるような置換がなければならないので，これはあり得ない． □

正しい漸近的増大度は，（上からは）ジョエル・スペンサー，（下からは）エルデシュ，セメレディ，トロッターによって，

$$\dim(K_n) \ \sim \ \log_2 \log_2 n + (\frac{1}{2} + o(1)) \log_2 \log_2 \log_2 n$$

と与えられた．しかしこれで話は終わりではない．ごく最近，モリスとホステンは，$\dim(K_n)$ の**厳密**な値を原理的に定める方法を発見した．彼らの結果と計算機を使えば，余白にある値を得ることができる．まったく，これには驚いてしまう！ 1422564 の大きさの置換がいくつあるか，ちょっと考えてみるとよい．$K_{1422564}$ の表現に必要な置換が 7 つか 8 つかを，どうやって決めるというのか？

$\dim(K_n) \leq 4 \iff n \leq 12$

$\dim(K_n) \leq 5 \iff n \leq 81$

$\dim(K_n) \leq 6 \iff n \leq 2646$

$\dim(K_n) \leq 7 \iff n \leq 1422564$

3. 和

ポール・エルデシュは，鳩の巣原理の次の素敵な応用はアンドリュー・ヴァゾニュイとマルタ・スヴェドによる，と言っている．

主張. 必ずしも異ならなくてよい n 個の整数 $a_1, \dots, a_n$ が与えられているとする. そのとき, 連続した数の集合 $a_{k+1}, a_{k+2}, \dots, a_\ell$ で, その和 $\sum_{i=k+1}^{\ell} a_i$ が n の倍数であるものが存在する.

証明のために, $N = \{0, a_1, a_1 + a_2, \dots, a_1 + a_2 + \dots + a_n\}$ と $R = \{0, 1, \dots, n-1\}$ とおき, 写像 $f : N \to R$ を考える. ただし, $f(m)$ は m を n で割った余りとする. $|N| = n + 1 > n = |R|$ だから, 同じ余りを持つ 2 つの和 $a_1 + \dots + a_k$, $a_1 + \dots + a_\ell$ $(k < \ell)$ が存在することになる. ここで, 前の方の和が空の和であることもあって, そのときは 0 である. これから

$$\sum_{i=k+1}^{\ell} a_i = \sum_{i=1}^{\ell} a_i - \sum_{i=1}^{k} a_i$$

の余りが 0 であることがわかる. これで証明は終わり. □

2 通りに数えるという, 第 2 の原理に移ろう. これは次のような意味である.

2 重数え上げ

2 つの有限集合 R, C と部分集合 $S \subseteq R \times C$ が与えられているとする. $(p, q) \in S$ のときに, p と q は隣接すると言う. r_p で, $p \in R$ に隣接する元の数を表わし, c_q で, $q \in C$ に隣接する元の数を表わすと,

$$\sum_{p \in R} r_p = |S| = \sum_{q \in C} c_q \tag{3}$$

となる[1].

これもまた, 証明することは何もない. 第 1 の和は第 1 成分に従って S に属する対を分けていて, 第 2 の和は第 2 成分に従って S に属する対を分けているだけである.

[1] [訳註] 以下の行列表示に対応して, R は行 (row), C は列 (column) に対応している.

集合 S を図示する有効な方法がある．S の**隣接行列** $A=(a_{pq})$ を考えるのである．A の行と列はそれぞれ R と C の元によって番号付けられていて，

$$a_{pq} = \begin{cases} 1 & (p,q) \in S \text{ のとき} \\ 0 & (p,q) \notin S \text{ のとき} \end{cases}$$

とする．この枠組みでは，r_p は A の第 p 行の和であり，c_q は第 q 列の和になっている．それゆえ，(3) における第 1 の和は S の元を行で足したもの（A の中の 1 を数えたもの）であり，第 2 の和は列で足したものである．

次の例はこの対応をはっきりさせてくれる．$R = C = \{1, 2, \ldots, 8\}$ として，$S = \{(i,j) : i$ は j を割り切る $\}$ とおく．そのとき，余白の行列が得られる（1 だけ書いてある）．

R \ C	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2		1		1		1		1
3			1			1		
4				1				1
5					1			
6						1		
7							1	
8								1

4. 数ふたたび

左上の表を見よう．j 列にある 1 の数は j の約数の数であり，この数を $t(j)$ と書く．j を 1 から n まで動かしたときの**平均**として，この数 $t(j)$ がどれくらいの大きさかを考えよう．つまり，量

$$\bar{t}(n) = \frac{1}{n}\sum_{j=1}^{n} t(j)$$

を問題にするのである．

n	1	2	3	4	5	6	7	8
$\bar{t}(n)$	1	$\frac{3}{2}$	$\frac{5}{3}$	2	2	$\frac{7}{3}$	$\frac{16}{7}$	$\frac{5}{2}$

$\bar{t}(n)$ の最初の方の値．

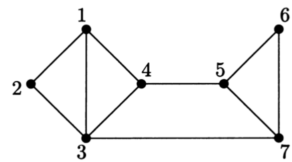
任意の n に対して，$\bar{t}(n)$ はどれ位の大きさだろうか？　ちょっと考えると，絶望的にも見える．素数 p に対しては $t(p) = 2$ となるが，2^k に対してなら大きな数 $t(2^k) = k+1$ が得られる．そんな風に，$t(n)$ は激しく飛び跳ねる関数であり，$\bar{t}(n)$ に対しても同じだという推測ができる．でも推測は間違いで，その反対が正しい！　2 つの方法で数えると，予期しない単純な解答が得られる．

整数 1 から n に対して（上のような）行列 A を考える．列に関して数えれば $\sum_{j=1}^{n} t(j)$ が得られる．第 i 行にはどれだけの 1 があるだろうか？　これは簡単で，1 は i の倍数である $1i, 2i, \ldots$ に対応しており，n を超えない最後の倍数は $\lfloor \frac{n}{i} \rfloor i$ である．それゆえ，

$$\bar{t}(n) = \frac{1}{n}\sum_{j=1}^{n} t(j) = \frac{1}{n}\sum_{i=1}^{n}\left\lfloor\frac{n}{i}\right\rfloor \le \frac{1}{n}\sum_{i=1}^{n}\frac{n}{i} = \sum_{i=1}^{n}\frac{1}{i}$$

である．ここで，和の各項で，$\lfloor\frac{n}{i}\rfloor$ から $\frac{n}{i}$ へ移るときの違いは 1 より小さい．それゆえ，平均したときの全体の違いもまた 1 より小さい．さて最後の和は n 番目の調和数で，粗っぽく言えば $\log n$ に等しく，その違いは 1 より小さい（14 ページ参照）．まとめると，次の注目すべき結果が得られる．「$t(n)$ はまったくバラバラなのに，平均 $\bar{t}(n)$ の振る舞いは美しく，$\bar{t}(n) \sim \log n$ を満たし，その誤差は 2 より小さい．」

5. グラフ



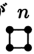
G を有限単純グラフで，頂点集合を V，辺の集合を E とする．第 10 章で，頂点 v の**次数** $d(v)$ を，v を端点とする辺の数として定義した．図の例では，頂点 $1, 2, \ldots, 7$ の次数はそれぞれ $3, 2, 4, 3, 3, 2, 3$ である．

グラフ理論のほとんどすべての本は，

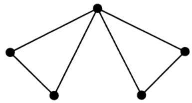
$$\sum_{v\in V} d(v) = 2|E| \tag{4}$$

という結果（これにはすでに第 10 章と第 16 章で出会っている）から始めている．証明のために $S \subseteq V \times E$ を考える．ここで，S は，$v \in V$ が $e \in E$ の端点であるような対 (v, e) の集合である．S を 2 通りに数えると，一方では，あらゆる頂点に対して $d(v)$ 回数えるので $\sum_{v\in V} d(v)$ であり，他方，各辺は 2 つの端点を持つので，$2|E|$ となる．　□

結果 (4) は単純だが，また多くの重要な結論を持っていて，そのいくつかについては以下で述べることになる．この節では，グラフに関する**極値問題**についての次の美しい応用を選ぶことにしよう．問題はこうである．

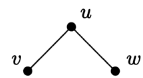
> **$G = (V, E)$ が n 個の頂点を持ち，どんな長さ 4 のサイクル，つまり， という形の部分グラフを含まないとする（これを C_4 条件と呼ぶ）．G は最大でいくつの辺を持ち得るか？**

たとえば，次ページの余白にある 5 頂点上のグラフは 4 サイクルを持



たず，6つの辺を持っている．5頂点上では辺の最大数が6であり，このグラフが4サイクルを持たない5頂点上のグラフで6つの辺を持つ唯一のグラフであることは，読者も容易に示せるだろう．

一般の問題に取り組んでみよう．G を4サイクルを持たない n 頂点上のグラフとする．上のように u の次数を $d(u)$ と書く．さて，次の集合 S を2通りに数えてみる．S は，対 $(u,\{v,w\})$ で，u が v と w に隣接し，$v \neq w$ であるものの集合であるとする．言い換えると，



が現れる回数を数えるのである．u について足せば，$|S| = \sum_{u\in V}\binom{d(u)}{2}$ が得られる．一方，あらゆる対 $\{v,w\}$ は（C_4 条件から）高々1つの隣接頂点を持つ．それゆえ，$|S| \leq \binom{n}{2}$ であって，

$$\sum_{u\in V}\binom{d(u)}{2} \;\leq\; \binom{n}{2}$$

つまり

$$\sum_{u\in V} d(u)^2 \;\leq\; n(n-1) + \sum_{u\in V} d(u) \tag{5}$$

という結論が得られる．

次に（そしてこれはこの種の極値問題にとって全く典型的なのだが），ベクトル $(d(u_1),\ldots,d(u_n))^T$ と $(1,1,\ldots,1)^T$ にコーシー–シュヴァルツの不等式を使うと，

$$\Big(\sum_{u\in V} d(u)\Big)^2 \;\leq\; n\sum_{u\in V} d(u)^2$$

が得られ，それゆえ (5) によって

$$\Big(\sum_{u\in V} d(u)\Big)^2 \;\leq\; n^2(n-1) + n\sum_{u\in V} d(u)$$

が得られる．(4) を代入すると，

$$4\,|E|^2 \;\leq\; n^2(n-1) + 2n\,|E|$$

つまり，

$$|E|^2 - \frac{n}{2}|E| - \frac{n^2(n-1)}{4} \quad \le \quad 0$$

が得られる．対応する 2 次方程式を解けば，イストヴァン・レイマンによる次の結果が得られたことになる．

定理． n **頂点上のグラフ** G **が 4 サイクルを含まなければ，**

$$|E| \quad \le \quad \left\lfloor \frac{n}{4}\left(1+\sqrt{4n-3}\right) \right\rfloor \tag{6}$$

である．

$n=5$ のとき，これから $|E| \le 6$ となるが[2]，上のグラフは等式が成り立ち得ることを示している．

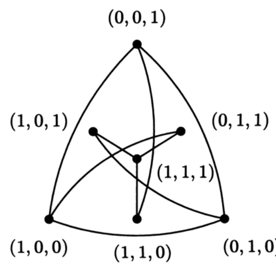
このように，2 通りに数えることで，辺の数の上界が簡単に得られたのである．しかし，この上界 (6) は一般に言ってどれくらいよいのだろうか？ 以下の美しい例 ([2], [3], [6]) からは，これがほとんどギリギリであることがわかる．このような問題の場合には，有限幾何が道を示してくれることも多い．

例を示すに際して，読者が，素数 p を法とする整数のなす有限体 $\mathbb{Z}_p$ (27 ページ参照) に慣れていることを仮定する．$\mathbb{Z}_p$ 上の 3 次元ベクトル空間 X を考える．X から次のグラフ G_p を作る．G_p の頂点は 1 次元部分空間 $[\boldsymbol{v}] = \mathrm{span}_{\mathbb{Z}_p}\{\boldsymbol{v}\}$, $\boldsymbol{0} \ne \boldsymbol{v} \in X$ であり，そのような 2 つの部分空間 $[\boldsymbol{v}]$, $[\boldsymbol{w}]$ を，

$$\langle \boldsymbol{v}, \boldsymbol{w} \rangle \ = \ v_1w_1 + v_2w_2 + v_3w_3 \ = \ 0$$

を満たすとき辺で結ぶ．このことは部分空間から $\boldsymbol{0}$ でないどんなベクトルをとるかには関係がないことに注意する．幾何の言葉では，このような頂点は $\mathbb{Z}_p$ 上の射影平面の点であり，$[\boldsymbol{w}]$ と $[\boldsymbol{v}]$ が隣接するのは，$\boldsymbol{w}$ が $\boldsymbol{v}$ の極線上にあるときである．

たとえば，グラフ G_2 は 4 サイクルを持たず，9 つの辺を持ち，(6) で与えられる上界 10 にほとんど届いている[3]．このことが任意の素数に対



グラフ G_2：頂点は 0 でないすべての 3 つ組 (x, y, z) で，7 つある．

[2] ［訳註］ $\frac{5}{4}\left(1+\sqrt{4\cdot 5-3}\right) < 7 \Leftrightarrow 5\sqrt{17} < 23$.

[3] ［訳註］ G_2 は $\mathbb{Z}_2$ 上の射影平面から作られるので，$2=0$ であることに注意．このことから $(1,1,1)$ の次数が 3 になる．

して正しいことを示したい．

まず，G_p が C_4 条件を満たすことを証明する．もし $[\boldsymbol{u}]$ が $[\boldsymbol{v}]$ とも $[\boldsymbol{w}]$ とも隣接していれば，$\boldsymbol{u}$ は 1 次方程式系

$$\begin{aligned} v_1x + v_2y + v_3z &= 0 \\ w_1x + w_2y + w_3z &= 0 \end{aligned}$$

の解である．$\boldsymbol{v}$ と $\boldsymbol{w}$ が 1 次独立なので，解空間の次元は 1 となって，それゆえ，共通の隣接頂点である $[\boldsymbol{u}]$ は一意的である．

次に，G_p がいくつの頂点を持つかを問題にする．またも 2 重数え上げである．空間 X は p^3-1 個の $\mathbf{0}$ でないベクトルを含んでいる．あらゆる 1 次元部分空間は $\mathbf{0}$ でない $p-1$ 個のベクトルを含むので，X には $\frac{p^3-1}{p-1} = p^2+p+1$ の 1 次元部分空間があることになり，つまり，G_p は $n = p^2+p+1$ 個の頂点を持つことになる．同じように，どんな 2 次元部分空間も $\mathbf{0}$ でない p^2-1 個 のベクトルを含み，それゆえ $\frac{p^2-1}{p-1} = p+1$ の 1 次元部分空間を含む．

残っているのは，G_p の中の辺の数，つまり，(4) から同じことになるが，次数を決めることである．G_p の構成から，$[\boldsymbol{u}]$ に隣接する頂点は，方程式

$$u_1x + u_2y + u_3z = 0 \tag{7}$$

の解である．(7) の解空間は 2 次元部分空間であり，それゆえ $[\boldsymbol{u}]$ に隣接する頂点は $p+1$ 個ある．しかし，気をつけなければいけないのは，$[\boldsymbol{u}]$ 自身が (7) の解であることもあり得るということである．この場合には，$[\boldsymbol{u}]$ に隣接するのは p 個の頂点しかない．

まとめると，次の結果が得られる．$\boldsymbol{u}$ が $x^2+y^2+z^2=0$ で与えられる錐の上にあれば，$d([\boldsymbol{u}]) = p$ であり，そうでなければ，$d([\boldsymbol{u}]) = p+1$ である．だから，残っているのは，

$$x^2+y^2+z^2=0$$

という錘の上にある 1 次元部分空間の数を求めることである．結果を予想して，すぐにそれを証明することにしよう．

主張．方程式 $x^2+y^2+z^2=0$ の解 (x,y,z) はちょうど p^2 個で，それゆえ（$\mathbf{0}$ 解を除いて）G_p の中の次数 p の頂

点はちょうど $\frac{p^2-1}{p-1}=p+1$ 個である.

これで G_p の解析は完成する．次数 p の頂点が $p+1$ 個あるので，次数 $p+1$ の頂点は $(p^2+p+1)-(p+1)=p^2$ 個である．(4) を使うと，

$$\begin{aligned}|E| &= \frac{(p+1)p}{2}+\frac{p^2(p+1)}{2} \;=\; \frac{(p+1)^2p}{2}\\ &= \frac{(p+1)p}{4}(1+(2p+1)) \;=\; \frac{p^2+p}{4}(1+\sqrt{4p^2+4p+1})\end{aligned}$$

が得られる．$n=p^2+p+1$ とおけば，最後の等式は

$$|E|=\frac{n-1}{4}(1+\sqrt{4n-3})$$

となって，これはもうほとんど (6) と一致している．

今度は上の主張を証明しよう．以下の議論は，対称行列とその固有値を含む線形代数の美しい応用になっている．第 31 章でも同じ方法が出てくるが，偶然の一致ではない．両方の証明とも，エルデシュ，レニイ，ソスの同じ論文にある．

X の 1 次元部分空間を，上のように，どの 2 つも 1 次独立なベクトル $\boldsymbol{v}_1,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_{p^2+p+1}$ で表わす．同じように，2 次元部分空間も同じベクトルの集合で表わすこともできる．ここで，$\boldsymbol{u}=(u_1,u_2,u_3)^T$ に対応する部分空間は，(7) でのように，方程式 $u_1x+u_2y+u_3z=0$ の解の集合である.（もちろん，これは線形代数の双対原理に過ぎない.）それゆえ，(7) により，$\boldsymbol{v}_i$ によって表わされる 1 次元部分空間が $\boldsymbol{v}_j$ で表わされる 2 次元部分空間に含まれるのは，$\langle\boldsymbol{v}_i,\boldsymbol{v}_j\rangle=0$ のとき，かつそのときに限る．

今度は以下のように定義される，サイズが $(p^2+p+1)\times(p^2+p+1)$ の行列 $A=(a_{ij})$ を考える．A の行と列は，

$$a_{ij} \;=\; \begin{cases}1 & \langle\boldsymbol{v}_i,\boldsymbol{v}_j\rangle=0 \text{ のとき}\\ 0 & \text{その他}\end{cases}$$

を満たすものとして，$\boldsymbol{v}_1,\ldots,\boldsymbol{v}_{p^2+p+1}$ に対応している（行と列に同じ番号をつけている）．こうして，A は実対称行列で，$\langle\boldsymbol{v}_i,\boldsymbol{v}_i\rangle=0$ のとき，つまり，$\boldsymbol{v}_i$ が錐 $x^2+y^2+z^2=0$ の上にあるとき，$a_{ii}=1$ である．こうして，残っているのは

$$A=\begin{pmatrix}0&1&1&1&0&0&0\\1&0&1&0&1&0&0\\1&1&0&0&0&1&0\\1&0&0&1&0&0&1\\0&1&0&0&1&0&1\\0&0&1&0&0&1&1\\0&0&0&1&1&1&0\end{pmatrix}$$

G_2 に対する行列.

$$\mathrm{trace}\, A \;=\; p+1$$

を示すことだけである．

線形代数から，トレースが固有値の和に等しいことを知っている．そしてここにもトリックがある．A は複雑そうに見えるが，行列 A^2 の解析は容易である．次の 2 つの事実に注意する．

- A のどんな行にも $p+1$ 個の 1 がある．これから $p+1$ が A の固有値であることがわかる．というのは，$\mathbf{1}$ を成分がすべて 1 であるベクトルとすると，$A\mathbf{1} = (p+1)\mathbf{1}$ となるからである．

- 2 つの異なる行 $\boldsymbol{v}_i, \boldsymbol{v}_j$ に対して，両方の行に 1 がある列（$\boldsymbol{v}_i, \boldsymbol{v}_j$ によって張られる一意的な部分空間に対応する列）がちょうど 1 つある．

これらの事実を使うと，

$$A^2 = \begin{pmatrix} p+1 & 1 & \cdots & 1 \\ 1 & p+1 & & \vdots \\ \vdots & & \ddots & \\ 1 & \cdots & & p+1 \end{pmatrix} \;=\; pI \;+\; J$$

であることがわかる．ここで，I は単位行列で，J はすべてが 1 の行列である．さて，J の固有値は（重複度 1 の）p^2+p+1 と（重複度 p^2+p の）0 である．それゆえ，A^2 の固有値は（重複度 1 の）$p^2+2p+1 = (p+1)^2$ と（重複度 p^2+p の）p である．A は実対称行列で，対角化可能であるから，A の固有値は $p+1$ または $-(p+1)$ と，p^2+p 個の $\pm\sqrt{p}$ という形であることがわかる．上の事実 1 から，最初の固有値は $p+1$ でないといけない．$\sqrt{p}$ の重複度が r で，$-\sqrt{p}$ の重複度が s であるとすれば，

$$\mathrm{trace}\, A \;=\; (p+1) + r\sqrt{p} - s\sqrt{p}$$

となる．と，ここが急所で，トレースは整数なのだから，$r = s$ でなければならず，$\mathrm{trace}\, A = p+1$ である． □

6. シュペルナーの補題

1911年にルイツェン・ブラウエルは有名な固定点定理を発表した.

n 次元球体から自分自身へのあらゆる連続写像 $f: B^n \longrightarrow B^n$ は，固定点（$f(\boldsymbol{x}) = \boldsymbol{x}$ を満たす点 $\boldsymbol{x} \in B^n$）を持つ.

1次元のときは，区間に対する問題になって，中間値の定理から容易に得られるが，高次元のときは，ブラウエルの証明にはいくらか精巧な機構が必要である．したがって，1928年に（当時23歳の）若いエマニュエル・シュペルナーが，ある単純な組合せ論的な結果を示し，その結果からブラウエルの固定点定理と全単射な連続写像の下での次元の不変性を導き出すことができたときには，驚きを持って迎えられた．その上，シュペルナーの巧妙な補題は同じように美しい証明とも似合っている．それは2重数え上げそのものである.

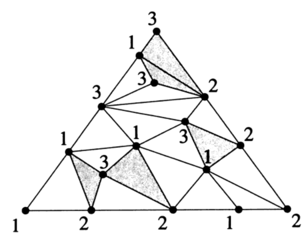
シュペルナーの補題と，その結果としてブラウエルの定理を，最初の興味ある場合として $n=2$ 次元の場合を述べる.（次元に関する帰納法によって）証明を高次元に拡張することには，読者も困難を感じないで済むだろう.

シュペルナーの補題.

頂点 V_1, V_2, V_3 を持つある「大きな」三角形が三角形分割されている（つまり，辺と辺で合わさった有限個の「小さい」三角形に分割されている）とする.

三角形分割の頂点には，集合 $\{1,2,3\}$ からの色がついており,（各 i に対して）V_i には色 i が，V_i から V_j $(i \neq j)$ への辺の上の頂点には色 i か j だけが，内部の頂点には 1, 2, 3 の任意の色が許されるとする.

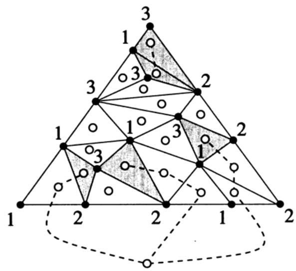
そのとき，三角形分割の中に「3色」の，つまり異なる3つの色を持つ小さい三角形が存在しなければならない.



異なる3色を持つ三角形に影をつけてある.

■ **証明.** より強い主張「3色の三角形の数が0でないだけでなく，つねに奇数である」を証明することにする.

三角形分割の双対グラフを考えるが，そのすべての辺をとるのではなく,（異なる）1と2の色の端点を持つ辺を横切るものだけをとることにする．こうして得られる「部分双対グラフ」では，3色三角形に対応するすべての頂点の次数は1で，1と2の2色が現れる三角形に対しては



次数2で，1と2の両方の色を持たない三角形に対しては次数0である．こうして，3色の三角形だけが奇数次（次数1）の頂点に対応している．

しかしながら，三角形分割の外側に対応する双対グラフの頂点は奇数次である．実際，V_1 から V_2 への大きな辺に沿っての1と2の変化は奇数回である．こうして，部分双対グラフの奇数個の辺がこの大きな辺と交わり，他の大きな辺は1と2の両方の色を持ち得ない．

さて，(等式 (4) により) 任意の有限グラフの奇数次の頂点の数は偶数であるから，(考えている双対グラフの内部の奇数次の頂点に対応する) 3つの異なる色を持つ小さな三角形の数が奇数であることがわかる． □

この補題を使うと，容易にブラウエルの定理を導くことができる．

■ **（$n=2$ に対する）ブラウエルの固定点定理の証明．** Δ を，頂点 $\boldsymbol{e}_1 = (1,0,0)$, $\boldsymbol{e}_2 = (0,1,0)$, $\boldsymbol{e}_3 = (0,0,1)$ を持つ，$\mathbb{R}^3$ の三角形とする．Δ は2次元球体 B_2 と同相だから，あらゆる連続写像 $f : \Delta \longrightarrow \Delta$ が固定点を持つことを証明すればよい．

三角形分割 $\mathcal{T}$ の中の辺の最大の長さを $\delta(\mathcal{T})$ と表わす．Δ の三角形分割の無限列 $\mathcal{T}_1, \mathcal{T}_2, \ldots$ で，最大直径[4] $\delta(\mathcal{T}_k)$ の列が0に収束するものを容易に作ることができる．そのような列は具体的な構成によって，つまり帰納的に，たとえば，$\mathcal{T}_{k+1}$ を $\mathcal{T}_k$ の重心細分としてとることによって得ることができる．

これらの各三角形分割ごとに，頂点の3色の彩色を $\lambda(\boldsymbol{v}) = \min\{i : f(\boldsymbol{v})_i < v_i\}$，つまり，$f(\boldsymbol{v}) - \boldsymbol{v}$ の第 i 座標が負になるような最小の添え字 i を $\lambda(\boldsymbol{v})$ とすることによって定義する．f が固定点を持たないと仮定するなら，この彩色は確かに定義になっている．このことを見るために，あらゆる $\boldsymbol{v} \in \Delta$ は平面 $x_1 + x_2 + x_3 = 1$ に属し，$\sum_i v_i = 1$ を満たすことに注意する．だから，$f(\boldsymbol{v}) \neq \boldsymbol{v}$ であれば，$f(\boldsymbol{v}) - \boldsymbol{v}$ の少なくとも1つの座標が負（そして少なくとも1つは正）でなければならない．

この彩色がシュペルナーの補題の仮定を満たすことを確かめよう．まず，頂点の色 $\boldsymbol{e}_i$ は i になる．というのは，$f(\boldsymbol{e}_i) - \boldsymbol{e}_i$ の成分で負になり得るのは i 番目だけである．さらに，$\boldsymbol{v}$ が $\boldsymbol{e}_i$ の対辺上にあれば，$v_i = 0$ であり，だから $f(\boldsymbol{v}) - \boldsymbol{v}$ の第 i 成分は負になり得ず，それゆえ，$\boldsymbol{v}$ の

[4] ［訳註］平面の閉集合 T の直径とは，T の属する2点間の距離の最大値であり，T が三角形のときは最大辺の長さになる．だから，$\delta(\mathcal{T})$ は三角形分割 $\mathcal{T}$ の三角形の直径のうちで最大のものとなる．

色は i にはなり得ない．

シュペルナーの補題から，今度は，各三角形分割 $\mathcal{T}_k$ において，$\lambda(\boldsymbol{v}^{k:i}) = i$ であるような 3 色三角形 $\{\boldsymbol{v}^{k:1}, \boldsymbol{v}^{k:2}, \boldsymbol{v}^{k:3}\}$ が存在することがわかる．点列 $(\boldsymbol{v}^{k:1})_{k\geq 1}$ は必ずしも収束しないが，単体 Δ はコンパクトなので，ある部分列は極限点を持つ．三角形分割の列 $\mathcal{T}_k$ を対応する部分列に取り換えて（簡単のためにこれも $\mathcal{T}_k$ と書く），$(\boldsymbol{v}^{k:1})_k$ がある点 $\boldsymbol{v} \in \Delta$ に収束すると仮定することができる．さて，$\boldsymbol{v}^{k:2}$ と $\boldsymbol{v}^{k:3}$ から $\boldsymbol{v}^{k:1}$ までの距離は高々網目の長さ $\delta(\mathcal{T}_k)$ であり，これは 0 に収束する．こうして，列 $(\boldsymbol{v}^{k:2})$ と $(\boldsymbol{v}^{k:3})$ は同じ点 $\boldsymbol{v}$ に収束する．

しかし，$f(\boldsymbol{v})$ はどこにあるのだろうか？ すべての k に対して，$f(\boldsymbol{v}^{k:1})$ の第 1 座標が $\boldsymbol{v}^{k:1}$ の第 1 座標より小さいことはわかっている．ところで，f は連続なので，$f(\boldsymbol{v})$ の第 1 座標は $\boldsymbol{v}$ の第 1 座標より小さいか等しいことが導かれる．同じ理由は第 2 座標と第 3 座標に対しても有効である．こうして，$f(\boldsymbol{v}) - \boldsymbol{v}$ のどの座標も正にはなれないが，これはすでに見たように，$f(\boldsymbol{v}) \neq \boldsymbol{v}$ という仮定に矛盾している． □

参考文献

[1] L. E. J. ブラウエル：「多様体の写像について」(*Über Abbildungen von Mannigfaltigkeiten*), Math. Annalen **71** (1912), 97-115.

[2] W. G. ブラウン：「トムセン・グラフを含まないグラフについて」(*On graphs that do not contain a Thomsen graph*), Canadian Math. Bull. **9** (1966), 281-285.

[3] P. エルデシュ，A. レニイ，V. ソス：「グラフ理論のある問題について」(*On a problem of graph theory*), Studia Sci. Math. Hungar. **1** (1966), 215-235.

[4] P. エルデシュ，G. シェッカーズ：「幾何学における 1 つの組合せ問題」(*A combinatorial problem in geometry*), Compositio Math. (1935), 463-470.

[5] S. ホステン，W. D. モリス：「完全グラフの順序次元」(*The order dimension of the complete graph*), Discrete Math. **201** (1999), 133-139.

[6] I. レイマン：「K. ザランキエヴィッツの問題について」(*Über ein Problem von K. Zarankiewicz*), Acta Math. Acad. Sci. Hungar. **9** (1958), 269-273.

[7] J. スペンサー：「単純順序の極大ごちゃまぜ集合」(*Minimal scrambling sets of simple orders*), Acta Math. Acad. Sci. Hungar. **22** (1971), 349-353.

[8] E. シュペルナー：「次元数と領域の不変性に対する新しい証明」(*Neuer Beweis für die Invarianz der Dimensionszahl und des Gebietes*), Abh. Math. Sem. Hamburg **6** (1928), 265-272.

[9] W. T. トロッター：『組合せ論と半順序集合：次元論』(*Combinatorics and Partially Ordered Sets: Dimension Theory*), John Hopkins University Press, Baltimore and London 1992.

第22章　有限集合に関する有名な3つの定理


エマニュエル・シュペルナー

この章では，組合せ論の基本的なテーマである，有限集合 $N = \{1, 2, \dots, n\}$ の部分集合の作る特殊な族 $\mathcal{F}$ の性質や大きさを問題とする．この分野での古典になっている2つの結果である，シュペルナーの定理とエルデシュ–コー–ラドーの定理から始めよう．この2つの結果の共通点は，何度も繰り返して証明され，それぞれ組合せ的集合論の新しい分野の始まりとなったということにある．どちらの定理にとっても，帰納法が自然に見えるが，これから述べる議論は全く異なったもので，実に素晴らしい発想のものである．

1928年にエマニュエル・シュペルナーは次の問題を問いかけ，そして解いた．集合 $N = \{1, 2, \dots, n\}$ が与えられているとする．N の部分集合の族 $\mathcal{F}$ は，$\mathcal{F}$ のどんな集合も族 $\mathcal{F}$ の別の集合を含まないとき，**反対鎖**と呼ばれる．最大の反対鎖の大きさはいくつだろうか？ 明らかに，すべての k 集合のなす族 $\mathcal{F}_k$ は反対鎖の性質を持ち，$|\mathcal{F}_k| = \binom{n}{k}$ である．2項係数の最大値を見ると（16ページ参照），大きさが $\binom{n}{\lfloor n/2 \rfloor} = \max_k \binom{n}{k}$ の反対鎖が存在するという結論が得られる．そこで，これ以上大きなものがないというのが，シュペルナーの定理である．

定理 1. ***n* 集合の最大の反対鎖の大きさは $\binom{n}{\lfloor n/2 \rfloor}$ である．**

■ **証明.** 多くある証明の中で，おそらく以下に述べるリューベルの証明がもっとも短くかつエレガントなものだろう．$\mathcal{F}$ を任意の反対鎖とする．そのとき，$|\mathcal{F}| \le \binom{n}{\lfloor n/2 \rfloor}$ を示さなければならない．証明の鍵となるのは，部分集合の鎖 $\varnothing = C_0 \subset C_1 \subset C_2 \subset \cdots \subset C_n = N$ を考えることである．ここで，$i = 0, \dots, n$ に対して $|C_i| = i$ であるとする．鎖はど

れほどあるだろうか？ 明らかに，N の元を 1 つずつ加えていって鎖を得ることができるので，ちょうど N の置換と同じだけの鎖が存在する．つまり $n!$ 個ある．次に，集合 $A \in \mathcal{F}$ に対して，A を含むような鎖がいくつあるかを考えよう．これも易しい．$\varnothing$ から A を得るには，A の元を 1 つずつ加えていけばよいし，A から N までならば残りの元を加えていけばよい．こうして，A が k 個の元を含むなら，上に考えた鎖を合わせた対のすべてを考えることによって，欲しい鎖が $k!(n-k)!$ 個あることがわかる．$\mathcal{F}$ は反対鎖だから，$\mathcal{F}$ の異なる 2 元 A と B を通るような鎖が存在しないことがわかる．

証明を終えるために，m_k を $\mathcal{F}$ の中の k 集合の数とする．すると，$|\mathcal{F}| = \sum_{k=0}^{n} m_k$ となり，上の議論から，$\mathcal{F}$ のある元を通る鎖の数は

$$\sum_{k=0}^{n} m_k \, k! \, (n-k)!$$

となって，この表示はすべての鎖の数である $n!$ を超えることができない．それゆえ

$$\sum_{k=0}^{n} m_k \frac{k!(n-k)!}{n!} \leq 1, \qquad \text{つまり} \qquad \sum_{k=0}^{n} \frac{m_k}{\binom{n}{k}} \leq 1$$

と結論される．したがって，分母を最大の 2 項係数で置き換えれば，

$$\frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \sum_{k=0}^{n} m_k \leq 1, \qquad \text{つまり} \qquad |\mathcal{F}| = \sum_{k=0}^{n} m_k \leq \binom{n}{\lfloor n/2 \rfloor}$$

が得られ，証明が完成する．　□

n が偶数のときはすべての $\frac{n}{2}$ 集合の集合が，また n が奇数のときはすべての $\frac{n-1}{2}$ 集合と $\frac{n+1}{2}$ 集合の集合だけが，実際に最大の大きさを持つ反対鎖であることを確かめよ！

2 つ目の結果は全く性質の異なるものである．もう一度，集合 $N = \{1, \ldots, n\}$ を考える．部分集合族 $\mathcal{F}$ は，$\mathcal{F}$ の任意の 2 元が少なくとも 1 つの（N の）元を共有するとき，**交差族**と呼ばれる．最大の交差族のサイズが 2^{n-1} であることは，ほとんどすぐにわかる．$A \in \mathcal{F}$ であれば，補集合 $A^c = N \backslash A$ は，A と点を共有しないので，$\mathcal{F}$ に属すことはできない．それゆえ，交差族はすべての部分集合の数 2^n の半分までしか含むことができない．つまり，$|\mathcal{F}| \leq 2^{n-1}$ ということになる．一方，ある固定した点を含むすべての集合の族，たとえば，1 を含むすべての部分集合の族 $\mathcal{F}_1$ を考えると，明らかに $|\mathcal{F}_1| = 2^{n-1}$ であり，問題は解

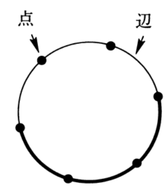
決したことになる．

しかし今度は,「交差族 $\mathcal{F}$ の集合が同じサイズ，たとえば k だとすると，どれくらい大きくなり得るだろうか？」という問題を考えてみよう．このような族を**交差 k 族**と呼ぼう．自明な場合を避けるために $n \geq 2k$ と仮定する．というのも，そうでなければ，任意の 2 つの k 集合は交わり，証明すべきことがないことになるからである．上のアイデアを使って，ある固定した元，たとえば 1，を含むすべての k 集合を考えれば，確かにそのような族 $\mathcal{F}_1$ が得られる．明らかに，$\mathcal{F}_1$ に属すすべての集合は，1 に $\{2, 3, \ldots, n\}$ の任意の $(k-1)$ 部分集合を加えて得られるので，$|\mathcal{F}_1| = \binom{n-1}{k-1}$ となる．もっとよくすることができるだろうか？ できないというのが答であり，それがエルデシュ–コー–ラドーの定理である．

定理 2. $n \geq 2k$ **のとき，**n **集合における交差** k **族の最大の大きさは** $\binom{n-1}{k-1}$ **である．**

ポール・エルデシュ，チャオ・コー，リチャード・ラドーは 1938 年にこの結果を発見していたが，23 年もの間公表されなかった．そのとき以来，多くの証明と変化形が与えられてきたが，ギューラ・カトナによる次の議論が特にエレガントである．

■ **証明.** 証明の鍵は次の簡単な補題である．それは一見すると，上の問題と全く無関係のように見える．円 C を n 個の点で n 個の辺に分けたとする．長さ k の弧とは，連続した $k+1$ 個の点とその間の k 個の辺からなるもののことである．



$n = 6$ に対する円 C．太線の辺は長さ 3 の弧を表している．

補題. $n \geq 2k$ **とし，長さ** k **の異なる弧** $A_1, \ldots, A_t$ **が** t **個与えられていて，どの 2 つの弧もある辺を共有しているとする．そのとき，**$t \leq k$ **である．**

補題の証明のために，まず，C の任意の点[1]は高々1 つの弧の端点であることに注意する．実際，もし A_i, A_j が共通の端点 v を持っていたら，(弧が異なっているから) 集合は反対の方向に動いていかないといけなくなる．しかし $n \geq 2k$ なので，1 つの辺を共有することは不可能である．A_1 を固定する．どんな A_i $(i \geq 2)$ も 1 つの辺を A_1 と共有するのだか

1 ［訳註］ここでは幾何的な意味での円の任意の点ではなく，上に与えた分点のことを言っている．

ら， A_i の 1 つの端点は A_1 の内点である．上で見たように，これらの端点は異なっていなければならないし，A_1 は $k-1$ 個の内点しか含まないので，A_1 以外には高々 $k-1$ 個の弧しか含み得ず，高々 k 個の弧しかないことが結論される． □

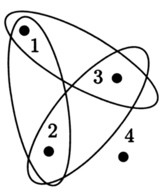
さて，エルデシュ–コー–ラドーの定理の証明に進もう．$\mathcal{F}$ を交差 k 族とする．上のように n 点と n 辺に分割された円 C を考える．任意の円順列 $\pi = (a_1, a_2, \ldots, a_n)$ をとり，数 a_i を C の辺の隣に，たとえば時計回りに書き込む．C 上の**連続**した k 個の数として現れる集合 $A \in \mathcal{F}$ の数を数えよう．$\mathcal{F}$ は交差族だから，上の補題により，そのような集合は高々 k 個である．これが任意の円順列に対して成り立ち，円順列は $(n-1)!$ 個あるので，このようにして，ある円順列の連続した元として現れる $\mathcal{F}$ の集合が，高々

$$k(n-1)!$$

個あることになる．ある固定した集合 $A \in \mathcal{F}$ を何重に数えただろうか？これは難しくない．A の k 個の元がある順序で連続的に現れるなら，A は π に現れる．それゆえ，A を連続的に書く方法は $k!$ 通りあり，残りの元を並べるのは $(n-k)!$ 通りである．だから，特定の集合 A はちょうど $k!(n-k)!$ 個の円順列に現れることになり，それゆえ

$$|\mathcal{F}| \leq \frac{k(n-1)!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} = \binom{n-1}{k-1} \quad (1)$$

となる． □



$n=4$, $k=2$ に対する交差族．

もう一度，ある固定した元を含む族が，唯一の交差 k 族なのかどうかを考えてみよう．これは確かに $n=2k$ では正しくない．たとえば，$n=4$, $k=2$ のとき，族 $\{1,2\},\{1,3\},\{2,3\}$ の大きさも $\binom{3}{1}=3$ である．もっと一般に，$n=2k$ のときは，次のようにして，大きさが $\frac{1}{2}\binom{n}{k}=\binom{n-1}{k-1}$ の極大交差 k 族が得られる．つまり，ある k 集合 A とその補集合 $N\backslash A$ からなるあらゆる集合対から任意に 1 つを入れることにすればよい．しかし $n>2k$ のときは，ある固定した元を含む特別な族が実際上ただ 1 つのものとなる．この証明は読者に委ねるが，実際に手を動かしてみて欲しい．

最後に，有限集合論ではおそらくもっとも重要な基本定理である第 3

の結果に移ろう．それは，1935年に証明されたフィリップ・ホールの「結婚定理」である．これは，今日マッチング理論と呼ばれるものへの扉を開いた定理である．その理論には広汎な種類の応用があり，そのうちのいくつかはこれ以降にも出てくるものである．

有限集合 X と，X の（必ずしも異なっていなくてよい）部分集合の集まり $A_1, \ldots, A_n$ を考える．点列 $x_1, \ldots, x_n$ を $\{A_1, \ldots, A_n\}$ の**異なる代表元の系**（SDR と略記する[2]）と呼ぶのは，x_i が X の異なる元であり，すべての i に対して $x_i \in A_i$ であるときである．もちろんこのような系 SDR が存在するとは限らない．たとえば，集合 A_i の 1 つが空集合なら系 SDR は存在しない．ホールの定理の内容は，SDR が存在するための厳密な条件である．

結果を与える前に，**結婚定理**と呼ぶ習慣についての人間的な説明をしておこう．少女の集合 $\{1, \ldots, n\}$ と少年の集合 X を考える．$x \in A_i$ であれば，少女 i と少年 x が結婚してもよいと思っていること，つまり，A_i は少女 i にとっての可能なマッチングの集合であるとする．そのとき，SDR は，あらゆる少女が彼女の好みの少年と結婚できる集団結婚を表している．

集合に戻って結果を述べよう．



「集団結婚式」

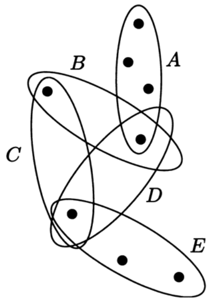
定理 3. **$A_1, \ldots, A_n$ を有限集合 X の部分集合の集まりとする．そのとき，異なる代表元の系が存在するのは，$1 \leq m \leq n$ に対して，どんな m 個の集合 A_i の和集合も m 個の元を含むとき，かつそのときに限る．**

条件は明らかに必要である．m 個の集合 A_i がその中に m より少ない個数の元しか含んでいないのなら，これらの m 個の集合が異なる代表元を持つことは，確かに不可能である．驚くべきなのは（普遍的な応用を持つ理由でもあるが），この明白な条件が十分条件でもあるということである．ホールの元々の証明はかなり複雑なもので，その後多くの別証が与えられてきた．その中でも，（イースターフィールドによるもので，ハルモスとヴォーガンによって再発見された）次のものがもっとも自然なものであろう．

■ **証明.** n に関する帰納法を使う．$n = 1$ のときは証明すべきことはな

[2] ［訳註］これは ‘system of distinct representatives’ の訳であり，頭文字をとって ‘SDR’ と呼んでいる．

い．$n > 1$ とし，$\{A_1, \ldots, A_n\}$ が定理の条件（この条件を (H) と略記する）を満たしているとする．ℓ $(1 \leq \ell < n)$ 個の集合 A_i の集まりは，その和集合の濃度が ℓ のとき，**臨界族**と呼ばれる．ここで，2 つの場合に分ける．



$\{B, C, D\}$ は臨界族．

場合 1：臨界族がない．

任意の元 $x \in A_n$ を選ぶ．X から x を除き，$A'_i = A_i \backslash x$ として，$A'_1, \ldots, A'_{n-1}$ という集まりを考える．臨界族がないのだから，どんな m 個の集合 A'_i の和集合も少なくとも m 個の元を含んでいる．それゆえ，n に関する帰納法から，$\{A'_1, \ldots, A'_{n-1}\}$ の SDR である $x_1, \ldots, x_{n-1}$ が存在し，$x_n = x$ を合わせれば，元の集まりに対する SDR になっている．

場合 2：臨界族が存在する．

集合の番号をつけ直して，$\{A_1, \ldots, A_\ell\}$ が臨界族だとしてよい．すると，$\bigcup_{i=1}^{\ell} A_i = \widetilde{X}$ の濃度は $|\widetilde{X}| = \ell$ となる．$\ell < n$ なので，帰納法から，$A_1, \ldots, A_\ell$ に対する SDR が存在する．つまり，すべての $i \leq \ell$ に対して $x_i \in A_i$ となるような $\widetilde{X}$ の番号付け $x_1, \ldots, x_\ell$ があることになる．

さて，残りの集まり $A_{\ell+1}, \ldots, A_n$ を考え，これらの集合から任意に m 個とる．$A_1, \ldots, A_\ell$ とこの m 個の集合との和集合は，条件 (H) により，少なくとも $\ell + m$ 個の元を含むので，この m 個の集合は $\widetilde{X}$ の外側に少なくとも m 個の元を含むことになる．言い換えれば，族

$$A_{\ell+1} \backslash \widetilde{X}, \; \ldots \; , A_n \backslash \widetilde{X}$$

に対して条件 (H) が満たされることになる．今度は帰納法から，$A_{\ell+1}, \ldots, A_n$ に対する SDR を $\widetilde{X}$ を避けながら与えることができる．これと $x_1, \ldots, x_\ell$ を合わせると，すべての集合 A_i に対する SDR が得られる．これで証明が完成した．　□

上に述べたように，ホールの定理は今や大きな分野になったマッチング理論 [6] の始まりであった．多くの変化形や細分化から，とくに魅力的な結果を述べておこう．読者は自分で証明してみることをお勧めする．

集合 $A_1, \ldots, A_n$ すべてが $k \geq 1$ の大きさを持ち，さらにどんな元も k 個以下の集合にしか含まれないと仮定する．そ

のとき，k 個の SDR が存在して，任意の i に対して，A_i の k 個の代表元は互いに異なっており，また，合わせると集合 A_i になっている．

結婚の可能性に関して新しい地平を開くであろう，美しい結果である．

参考文献

[1] T. E. イースターフィールド：「ある組合せ論的アルゴリズム」(*A combinatorial algorithm*), J. London Math. Soc. **21** (1946), 219-226.

[2] P. エルデシュ, C. コー, R. ラドー：「有限集合の系に対する交差定理」(*Intersection theorems for systems of finite sets*), Quart. J. Math. (Oxford), Ser. (2) **12** (1961), 313-320.

[3] P. ホール：「部分集合の表現について」(*On representatives of subsets*), Quart. J. Math. (Oxford) **10** (1935), 26-30.

[4] P. R. ハルモス, H. E. ヴォーガン：「結婚問題」(*The marriage problem*), Amer. J. Math. **72** (1950), 214-215.

[5] G. カトナ：「エルデシュ–チャオ・コー–ラドーの定理の簡単な証明」(*A simple proof of the Erdős-Chao Ko-Rado theorem*), J. Combinatorial Theory, Ser. B **13** (1972), 183-184.

[6] L. ロヴァース, M. D. プラマー：『マッチング理論』(*Matching Theory*), Akadémiai Kiadó, Budapest 1986.

[7] D. リューベル：「シュペルナーの定理の短い証明」(*A short proof of Sperner's theorem*), J. Combinatorial Theory **1** (1966), 299.

[8] E. シュペルナー：「有限集合の部分集合に関する定理」(*Ein Satz über Untermengen einer endlichen Menge*), Math. Zeitschrift **27** (1928), 544-548.

第23章　格子の道と行列式

数学の本質は定理を証明することで，だからそれが数学者のしていることである．つまり，彼らは定理を証明するのである．しかし，本当のことを言えば，生涯に一度，彼らが真実証明したいと思うのは**補題**なのである．たとえば，解析ならファトゥーの補題，数論ならガウスの補題，組合せ論ならバーンサイド–フロベニウスの補題のような補題である．

さて，どういうことがあれば，数学的な主張が真の意味で補題になるのだろうか？　第1に，広範な事例に，見かけからは何の関係もなさそうな問題にも適用できることである．第2に，その主張は，一旦わかれば，完全に明らかに見えるものでなければならない．それを読む者には一種の妬(ねた)みというか羨望の気持ちが湧くかも知れない．どうしてこれまでこれに気がつかなかったんだろう？　そして第3に，審美的な意味で，補題はその証明も込めて美しくあるべきである！

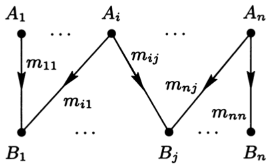
本章では，そのような数学的推論の素晴らしい一例である，イラ・ゲッセルとジェラール・ヴィアンノの補題を見ることにしよう．それは1985年に登場して，すぐに組合せ論的数え上げの古典になったものである．同様のことがそれ以前にベルント・リンドストレムによって得られている．

出発点は行列の行列式の，置換による通常の表示である．$M = (m_{ij})$ を実 $n \times n$ 行列とすると，

$$\det M \quad = \quad \sum_{\sigma} \operatorname{sign}\sigma \; m_{1\sigma(1)}\, m_{2\sigma(2)} \cdots m_{n\sigma(n)} \qquad (1)$$

である．ここで，σ は $\{1, 2, \ldots, n\}$ のすべての置換を動き，σ の符号

$(\mathrm{sign}\,\sigma)$ は σ が偶数個の互換の積であるか奇数個の互換の積であるかに従って 1 か -1 かである．



ここで，グラフに移ろう．より正確には**重み付きの有向 2 部**グラフにである．頂点 $A_1, \ldots, A_n$ は M の行を表し，$B_1, \ldots, B_n$ は列を表す．i と j の各対に対して，図のように，A_i から B_j への矢印を描き，重み m_{ij} を与える．

このグラフの言葉では，式 (1) には次のような説明ができる．

- 左辺は，(i, j) 成分が A_i から B_j への向きの（一意的な）道の重みであるような，**道の行列** M の行列式である．

- 右辺は，$\mathcal{A} = \{A_1, \ldots, A_n\}$ から $\mathcal{B} = \{B_1, \ldots, B_n\}$ への**頂点分離の道の系**全体にわたる重み付きの（符号付き）和である．そのような系 $\mathcal{P}_\sigma$ は，道

$$A_1 \to B_{\sigma(1)}, \quad \ldots \quad , A_n \to B_{\sigma(n)}$$

によって与えられ，道の系 $\mathcal{P}_\sigma$ の**重み**は個々の道の重みの積

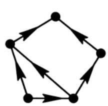
$$w(\mathcal{P}_\sigma) \;=\; w(A_1 \to B_{\sigma(1)}) \;\cdots\; w(A_n \to B_{\sigma(n)})$$

である．

この説明では，式 (1) は

$$\det M \;=\; \sum_\sigma \mathrm{sign}\,\sigma\; w(\mathcal{P}_\sigma)$$

となる．さて，何がゲッセルとヴィアンノの結果なのだろうか？ それは 2 部グラフから任意のグラフへの (1) の自然な一般化である．補題がそれほど広範に応用可能になるのはこの部分のおかげであり，さらに，証明が途方もなく単純でエレガントになるのである．


サイクルのない有向グラフ．

まず，必要な概念をまとめておこう．サイクルのない有限有向グラフ $G = (V, E)$ が与えられているとする．**サイクルがない**というのは，G の中に有向サイクルが存在しないという意味である．とくに，任意の 2 つの頂点 A と B を結ぶ有向な道は，長さ 0 の自明な道 $A \to A$ を含めても，有限個しかない．あらゆる辺 e には重み $w(e)$ がある．P が A から B への有向な道であれば，それを簡単に $P : A \to B$ と書くことにするが，P の重みを

$$w(P) \;=\; \prod_{e\in P} w(e)$$

と定義する．P が長さ 0 の道ならば，$w(P)=1$ であると定義する．

$\mathcal{A}=\{A_1,\ldots,A_n\}$ と $\mathcal{B}=\{B_1,\ldots,B_n\}$ を 2 つの n 頂点集合とし，$\mathcal{A}$ と $\mathcal{B}$ は交わりがあってもよいとする．$\mathcal{A}$ と $\mathcal{B}$ に**道の行列** $M=(m_{ij})$ を

$$m_{ij} \;=\; \sum_{P:A_i\to B_j} w(P)$$

として対応させる．$\mathcal{A}$ から $\mathcal{B}$ への**道の系** $\mathcal{P}$ は，置換 σ と n 本の道 $P_i : A_i \to B_{\sigma(i)}$ $(i=1,\ldots,n)$ とからなるもので，$\operatorname{sign}\mathcal{P} \;=\operatorname{sign}\sigma$ と書く．$\mathcal{P}$ の**重み**は道の重みの積

$$w(\mathcal{P}) \;=\; \prod_{i=1}^{n} w(P_i) \tag{2}$$

であり，道の系のすべての道の重みの積である．

最後に，道の系 $\mathcal{P}=(P_1,\ldots,P_n)$ が**頂点分離**であるとは，2 つずつ見て $\mathcal{P}$ の道が頂点が分離して（異なって）いることとする．

補題． $G=(V,E)$ をサイクルのない重み付きの有限有向グラフとし，$\mathcal{A}=\{A_1,\ldots,A_n\}$ と $\mathcal{B}=\{B_1,\ldots,B_n\}$ を 2 つの n 頂点集合とし，M を $\mathcal{A}$ から $\mathcal{B}$ への道の行列とする．そのとき，

$$\det M \;=\; \sum_{\mathcal{P}:\text{頂点分離の道の系}} \operatorname{sign}\mathcal{P}\; w(\mathcal{P}) \tag{3}$$

となる．

■ **証明．** 和 $\det(M)$ の代表的な項は $\operatorname{sign}\sigma\; m_{1\sigma(1)}\cdots m_{n\sigma(n)}$ で，

$$\operatorname{sign}\sigma\;\Big(\sum_{P_1:A_1\to B_{\sigma(1)}} w(P_1)\Big)\;\cdots\;\Big(\sum_{P_n:A_n\to B_{\sigma(n)}} w(P_n)\Big)$$

と書くことができる．σ に関して足し上げれば，(2) からすぐに

$$\det M \;=\; \sum_{\mathcal{P}} \operatorname{sign}\mathcal{P}\; w(\mathcal{P})$$

が得られる．ここで，$\mathcal{P}$ は $\mathcal{A}$ から $\mathcal{B}$ へのすべての道を動く（頂点が分

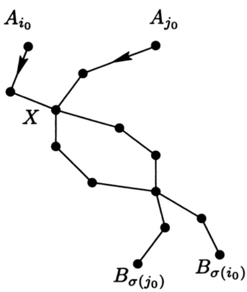
離していても，いなくても）．それゆえ，(3) まで行こうとすれば，示さなければならないのは

$$\sum_{\mathcal{P}\in N} \operatorname{sign}\mathcal{P}\ w(\mathcal{P}) \;=\; 0 \tag{4}$$

である．ここで，N は頂点が分離していないすべての道の系の集合である．そしてこのことは，際だって美しい議論によって実行される．つまり，(固定点を持たない) 対合 $\pi: N \to N$ で，$\mathcal{P}$ と $\pi\mathcal{P}$ に対して

$$w(\pi\mathcal{P}) \;=\; w(\mathcal{P}) \qquad \text{かつ} \qquad \operatorname{sign}\pi\mathcal{P} \;=\; -\operatorname{sign}\mathcal{P}$$

を満たすものを提示するのである．明らかに，こうであれば (4) が得られ，それから補題の公式 (3) が得られる．



対合 π はもっとも自然に定義される．$\mathcal{P} \in N$ を道 $P_i : A_i \to B_{\sigma(i)}$ を持つものとする．定義により，道の対のいくつかは交差している．

- i_0 を，P_{i_0} が他の道とある頂点を共有するような最小の添え字とする．
- X を道 P_{i_0} 上のその様な共通の頂点のうちで最初のものとする．
- j_0 を P_{j_0} が頂点 X を P_{i_0} と共有する最小の添え字 $(j_0 > i_0)$ とする．

そこで，新しい系 $\pi\mathcal{P} = (P'_1, \ldots, P'_n)$ を以下のように定義する．

- すべての $k \neq i_0, j_0$ に対しては $P'_k = P_k$ とおく．
- 新しい道 P'_{i_0} は A_{i_0} から X までは P_{i_0} に沿って行き，それから $B_{\sigma(j_0)}$ までは P_{j_0} に沿って行く．同じように，P'_{j_0} は A_{j_0} から X までは P_{j_0} に沿い，それから $B_{\sigma(i_0)}$ までは P_{i_0} に沿って行く．

明らかに $\pi(\pi\mathcal{P}) = \mathcal{P}$ である．なぜなら，添え字 i_0，頂点 X，添え字 j_0 は前と同じだからである．言い換えると，π を 2 度行えば，元の道 P_i に戻るのである．次に，$\pi\mathcal{P}$ と $\mathcal{P}$ はまったく同じ辺を使っているので，確かに $w(\pi\mathcal{P}) = w(\mathcal{P})$ となる．そして最後に，新しい置換 σ' は σ に互換 (i_0, j_0) を掛けたものだから，$\operatorname{sign}\pi\mathcal{P} = -\operatorname{sign}\mathcal{P}$ となる．これで証明は終わりである．□

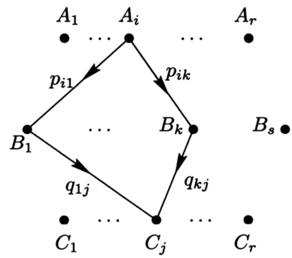
ゲッセル–ヴィアンノの補題は，適当なグラフを見ているだけで，行列

式のすべての基本性質を導くことに使うことができる．1つ特に驚くような例を考えることにしよう．行列式の積の規則の非常に役に立つ一般化であるビネ–コーシーの公式である．

定理． P が $(r \times s)$ 行列で，Q が $(s \times r)$ 行列 $(r \leq s)$ であれば，

$$\det(PQ) = \sum_{\mathcal{Z}} (\det P_{\mathcal{Z}})(\det Q_{\mathcal{Z}})$$

となる．ここで，$P_{\mathcal{Z}}$ は $\mathcal{Z}$ を列の集合とする P の $(r \times r)$ 小行列で，$Q_{\mathcal{Z}}$ は対応する $\mathcal{Z}$ を行の集合とする Q の $(r \times r)$ 小行列である．



■ **証明．** $\mathcal{A}$ と $\mathcal{B}$ 上の2部グラフを前と同じように P と対応させ，同様に $\mathcal{B}$ と $\mathcal{C}$ 上の2部グラフを Q と対応させる．今度は，余白の図に示したように繋いだグラフを考えてじっと見れば，$\mathcal{A}$ から $\mathcal{C}$ への道の行列 M の (i,j) 成分 m_{ij} がまさに $m_{ij} = \sum_k p_{ik}q_{kj}$ であり，$M = PQ$ となっていることがわかる．

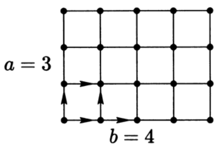
繋いだグラフにおける $\mathcal{A}$ から $\mathcal{C}$ への頂点分離の道の系は，それぞれ $\mathcal{A}$ から $\mathcal{Z}$ への系と $\mathcal{Z}$ から $\mathcal{C}$ への系の対であるから，sign $(\sigma\tau) =$ (sign σ) (sign τ) であることに注意すれば，結果は補題から直ちに得られる． □

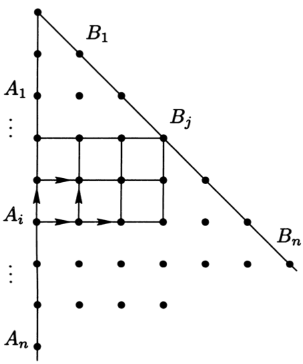
ゲッセル–ヴィアンノの補題はまた，数え上げる性質に行列式を関連付けるような多くの結果を産んでくれる．レシピはいつも同じである．行列 M をある道の行列と解釈し，(3) の右辺の計算をする．そのことの説明に，ゲッセルとヴィアンノがこの補題を考え付くもとになった，彼らが研究していた元々の問題を考えてみる．

$a_1 < a_2 < \cdots < a_n$ と $b_1 < b_2 < \cdots < b_n$ を自然数のつくる2つの集合とする．m_{ij} が2項係数 $\binom{a_i}{b_j}$ であるような行列 $M = (m_{ij})$ の行列式を計算したい．

言い換えると，ゲッセルとヴィアンノはパスカルの三角形から作られる任意の正方行列の行列式を求めていた．余白に描いたパスカルの三角形の太字の成分で与えられる

1							
1	1						
1	2	1					
1	**3**	3	**1**				
1	**4**	6	**4**	**1**			
1	5	10	10	5	1		
1	**6**	15	**20**	**15**	6	1	
1	7	21	35	35	21	7	1





$$\det\begin{pmatrix} \binom{3}{1} & \binom{3}{3} & \binom{3}{4} \\ \binom{4}{1} & \binom{4}{3} & \binom{4}{4} \\ \binom{6}{1} & \binom{6}{3} & \binom{6}{4} \end{pmatrix} = \det\begin{pmatrix} 3 & 1 & 0 \\ 4 & 4 & 1 \\ 6 & 20 & 15 \end{pmatrix}$$

のような行列の行列式である．

問題の解法の準備段階として，2 項係数を格子の道に結び付けるよく知られた結果を思い出そう．余白にあるような $a \times b$ 格子を考える．左下隅から右上隅への道で，各段階で上（北，North）か右（東，East）に行くことだけを許すものの数は $\binom{a+b}{a}$ である．

この証明は易しい．道はそれぞれ，b 回の東行き，a 回の北行きの歩みの任意の列からなり，a 個の N と b 個の E の，$a+b$ 個の文字の列からなる NENEEEN の形の列によってコード化される．このような列の数は，全体の $a+b$ 個の場所から文字 N の a 個の位置を選ぶ仕方の数であり，$\binom{a+b}{a} = \binom{a+b}{b}$ となる．

さて，余白の図を見よう．A_i は点 $(0, -a_i)$ に，B_j は $(b_j, -b_j)$ におかれている．

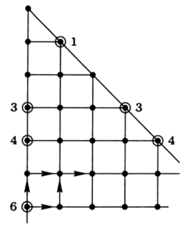
この格子の中で，北と東に進むことだけを許して，A_i から B_j へ行く道の数は，今証明した通り，$\binom{b_j+(a_i-b_j)}{b_j} = \binom{a_i}{b_j}$ となる．言い換えれば，2 項係数の行列 M はまさに，すべての辺の重みが 1 で，すべての辺が北か東かに向いているような有向格子グラフでの，$\mathcal{A}$ から $\mathcal{B}$ への道の行列となる．それゆえ，$\det M$ を計算するためにゲッセル–ヴィアンノの補題を使うことができる．ちょっと考えてみれば，$\mathcal{A}$ から $\mathcal{B}$ への，あらゆる頂点分離の道の系 $\mathcal{P}$ はすべての i に対して $P_i : A_i \to B_i$ である道からなっていなければならないことがわかる．こうして，唯一可能な置換は恒等置換で，その符号は sign $= 1$ であるから，美しい結果

$$\det\left(\binom{a_i}{b_j}\right) = \#\{\mathcal{A} \text{ から } \mathcal{B} \text{ への頂点分離の道の系}\}$$

が得られる．とくに，このことから，$\det M$ が常に非負であるという，自明とはほど遠い事実が得られる．というのも，等式の右辺は**あるものを数え**ているものだからである．実際，ゲッセル–ヴィアンノの補題から，$\det M = 0$ と，ある i に対して $a_i < b_i$ であることが同値であることが得られる．

たとえば，

$$\det\begin{pmatrix}\binom{3}{1} & \binom{3}{3} & \binom{3}{4}\\ \binom{4}{1} & \binom{4}{3} & \binom{4}{4}\\ \binom{6}{1} & \binom{6}{3} & \binom{6}{4}\end{pmatrix} = \#$$ 右の格子グラフにおける頂点分離の道の系

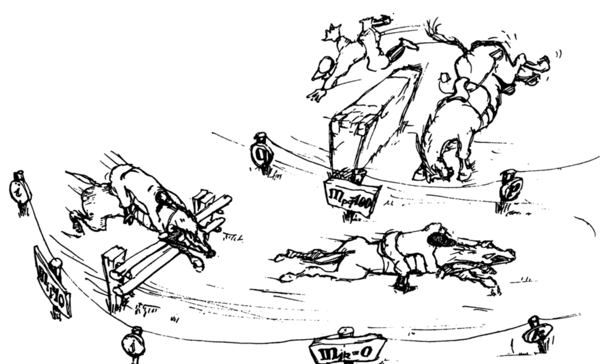


となる.

参考文献

[1] I. M. ゲッセル, G. ヴィアンノ:「2項行列式, 道, 鉤の長さ公式」(*Binomial determinants, paths, and hook length formulae*), Advances in Math. **58** (1985), 300-321.

[2] B. リンドストレム:「誘導マトロイドのベクトル表現について」(*On the vector representation of induced matroids*), Bulletin London Math. Soc. **5** (1973), 85-90.



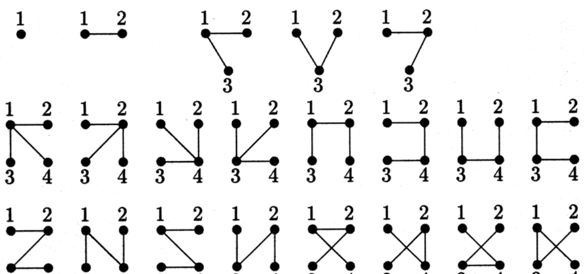
「格子の道」

第24章　木の数に対するケイリーの公式

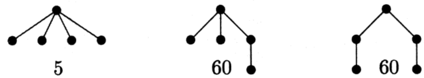


アーサー・ケイリー

数え上げ組合せ論のもっとも美しい公式の1つは，ラベル付きの木の数についてのものである．集合 $N = \{1, 2, \ldots, n\}$ を考える．この頂点集合の上に，いくつ異なる木を作ることができるだろうか？ この数を T_n と書こう.「手で」数えると，$T_1 = 1$, $T_2 = 1$, $T_3 = 3$, $T_4 = 16$ であることがわかる．その木は下の表に示したものである．



ラベル付きの木を考えていることに注意する．つまり，グラフの同型の意味では，位数3の木は1つしかないが，最初に内側の頂点を選ぶことによって3つのラベル付きの木が存在する．$n = 5$ に対しては，同型でない木は3つである．



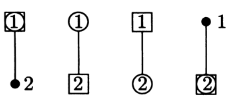
最初の木に対しては明らかに5つの異なるラベル付けがあり，第2と第3の木に対しては $\frac{5!}{2} = 60$ 個のラベル付けがあるので，$T_5 = 125$ となる．これでもう $T_n = n^{n-2}$ と予想するには十分だが，これがまさにケイリーの結果なのである．

定理．n 頂点上には n^{n-2} 個の異なるラベル付きの木が存在する．

この美しい公式には同じように美しい証明がある．そこでは，さまざまな組合せ論的な技巧と代数的な技巧が使われる．もっとも美しいと思われている証明を示す前に，3つの証明を大まかに述べておこう．

■ **第1の証明（全単射）．** 古典的でもっとも直接的な方法は，n 頂点上のすべての木の集合から，濃度が n^{n-2} であると知られている別の集合の上への全単射を見つけることである．$1 \le a_i \le n$ を満たすすべての順序列 $(a_1, \ldots, a_{n-2})$ の集合を思い付くのは自然なことである．そこで，あらゆる木 T の列 $(a_1 \ldots, a_{n-2})$ による一意的なコード化があればよい．そのようなコードはプリューファーによって発見され，グラフ理論のほとんどの本に載っている．

ここでは，ジョイアルによるもう1つの全単射を使った証明で，あまり知られていないが，同じようにエレガントで単純なものを述べよう．このために，$N = \{1, \ldots, n\}$ の木 t というだけでなく，2つの頂点を特別視したものを考える．一方を，**左端** ◯，もう一方を**右端** □と呼ぶが，その2点は一致してもよいとする．$\mathcal{T}_n = \{(t; \bigcirc, \square)\}$ をこの新しい集合とすると，明らかに $|\mathcal{T}_n| = n^2 T_n$ となる．



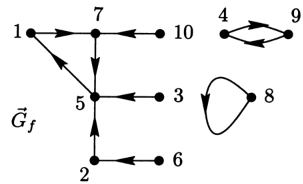
$\mathcal{T}_2$ の4つの木．

すると，$|\mathcal{T}_n| = n^n$ を証明するのがゴールとなる．さて，大きさが n^n であると知られている集合がある．N から N へのすべての写像の集合 N^N がそれである．そこで，N^N から $\mathcal{T}_n$ の上への全単射を見つけることができれば，公式が証明されたことになる．

$f : N \longrightarrow N$ を任意の写像とする．i から $f(i)$ へ矢印を描くことによって得られる有向グラフ $\vec{G}_f$ として f を表現する．

たとえば，写像

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 5 & 9 & 1 & 2 & 5 & 8 & 4 & 7 \end{pmatrix}$$



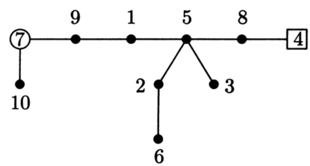
は余白の有向グラフによって表現される．

$\vec{G}_f$ の成分を見よう．各頂点からはちょうど1つの辺が出て行くのだから，各成分には同じ数の頂点と辺とがあり，それゆえ有向サイクルもちょうど1つある．$M \subseteq N$ をこれらのサイクルの頂点の集合とする．ちょっと考えてみれば，M が，f の M への制限が M 上の全単射として振る舞うような，N の**一意的な**極大部分集合であることがわかる．第1行の数 $a, b, \ldots, z$ が自然な順序になるようにして，$f|_M = \begin{pmatrix} a & b & \cdots & z \\ f(a) & f(b) & \cdots & f(z) \end{pmatrix}$ と書く．この第2行に従った，M の順序 $f(a), f(b), \ldots, f(z)$ を考え，$f(a)$ を左端，$f(z)$ を右端とする．

そこで，写像 f に対応する木 t を以下のように構成する．$f(a), \ldots, f(z)$ をこの順序で，$f(a)$ から $f(z)$ への**道**として描き，残りの頂点を $\vec{G}_f$ でと同じように補う（矢印はとる）．

上の例では，$M = \{1, 4, 5, 7, 8, 9\}$ となり，

$$f_M = \begin{pmatrix} 1 & 4 & 5 & 7 & 8 & 9 \\ 7 & 9 & 1 & 5 & 8 & 4 \end{pmatrix}$$



となって，余白に描かれた木 t が得られる．

この対応を反対にするのは，すぐにできる．木 t が与えられたら，左端から右端への一意的な道 P に目をつける．これから集合 M と写像 $f|_M$ がわかる．残りの対応 $i \to f(i)$ は，i から P への一意的な道に従って補えばよい．□

■ **第2の証明（線形代数）**．T_n を，完全グラフ K_n の全域木の数と考えることができる．さて，$V = \{1, 2, \ldots, n\}$ 上の任意の連結単純グラフ G を考え，全域木の数を $t(G)$ と表わす．すると，$T_n = t(K_n)$ である．次の有名な結果はキルヒホッフの**行列–木の定理**（[1] を参照）である．G の接続行列 $B = (b_{ie})$ を考える．その行は V で，列は E でラベル付けられ，$i \in e$ か $i \notin e$ に従って，$b_{ie} = 1$ か 0 と書く．G が連結だから，$|E| \geq n - 1$ となることに注意する．あらゆる列で，任意の仕

方で 2 つある 1 のうちの 1 つを -1 に置き換え（これが G の向き付けになる），この新しい行列を C と呼ぶ．すると，$M = CC^T$ は $(n \times n)$ 対称行列で，主対角線に次数 $d_1, \ldots, d_n$ が並ぶ．

命題． **すべての $i = 1, \ldots, n$ に対して $t(G) = \det M_{ii}$ となる．ここで，M_{ii} は M から第 i 行と第 i 列を取り除いて得られるものである．**

■ **証明．** 証明の鍵となるのは，前章で証明したビネ–コーシーの定理である．それは，P が $(r \times s)$ 行列で，Q が $(s \times r)$ 行列で，$r \leq s$ であるとき，$\det(PQ)$ は対応する $(r \times r)$ 小行列の行列式の積の和であるというものであった．ここで,「対応する」というのは，P の r 個の列と Q の r 個の行に対して同じ添え字をとるという意味である．

M_{ii} に対して，このことは

$$\det M_{ii} \;=\; \sum\nolimits_N \det N \cdot \det N^T \;=\; \sum\nolimits_N (\det N)^2$$

を意味している．ここで，N は $C \backslash \{\text{第}\, i\, \text{行}\}$ のすべての $(n-1) \times (n-1)$ 小行列を動く．N の $n-1$ 個の列は，n 個の頂点上の $n-1$ の辺を持つ G の部分グラフに対応しており，あと残っているのは

$$\det N = \begin{cases} \pm 1 & \text{これらの辺が木を張るとき} \\ 0 & \text{その他のとき} \end{cases}$$

を示すことである．

$n-1$ 個の辺が木を張らないとする．そのとき，i を含まない成分が存在する．この成分の対応する行を足し合わせると 0 になるので，それらが 1 次従属であること，それゆえ $\det N = 0$ であることがわかる．

今度は N の列が木を張ると仮定する．そのとき次数 1 の頂点 $j_1 \neq i$ が存在する．e_1 を，j_1 を端点とする辺とする．j_1, e_1 を除くと，$n-2$ 個の辺を持つ木が得られる．また，次数 1 の頂点 $j_2 \neq i$ と，j_2 を端点とする辺を e_2 が存在する．このようにして，$j_1, j_2, \ldots, j_{n-1}$ と $e_1, e_2, \ldots, e_{n-1}$ が $j_i \in e_i$ を満たすように決定されるまで続ける．今度は行と列を置換して，j_k を第 k 行に，e_k を第 k 列に持ってくる．構成により，$k < \ell$ に対しては $j_k \notin e_\ell$ だから，新しい行列 N' は下三角行列で，主対角線上の成分は ± 1 に等しい．こうして，$\det N = \pm \det N' = \pm 1$ となり，これで終わりである．



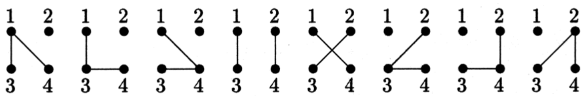
「木を数える標準的でない方法．それぞれの木に猫を登らせ，犬を歩かせて，犬が何度吠えるかを数える．」

$G = K_n$ という特殊な場合には，明らかに

$$M_{ii} = \begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & & -1 \\ \vdots & & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix}$$

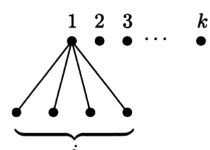
となり，簡単な計算で $\det M_{ii} = n^{n-2}$ がわかる[1]. □

■ **第3の証明（漸化式）.** 数え上げ組合せ論のもう1つの古典的な方法は漸化式を作って，この漸化式を帰納法で証明することである．以下のアイデアは本質的にリオーダンとレニイによる．正しい漸化式を見つけるために，(すでにケイリーの論文に現れていた）もっと一般な問題を考えよう．A を頂点の任意の k 集合とする．A の頂点が異なる木に現れるような，$\{1,\ldots,n\}$ 上の（ラベル付きの）森の数を $T_{n,k}$ と書く．明らかに，集合 A 自体がではなく，大きさ k だけが問題なのである．$T_{n,1} = T_n$ であることに注意しておく．



たとえば，$A = \{1,2\}$ に対しては $T_{4,2} = 8$ である．

$A = \{1,2,\ldots,k\}$ に対するこのような森 F を考え，余白の図で示したように，1 が i 個の頂点と隣接しているとする．1 を取り去れば，この i 個の頂点と $2,\ldots,k$ は $T_{n-1,k-1+i}$ 個の森を与える．$n-k$ 個の頂点から $1,\ldots,k$ 以外の i 個の頂点を任意に選ぶことができるのだから，$n \geq k \geq 1$ に対して，



$$T_{n,k} = \sum_{i=0}^{n-k} \binom{n-k}{i} T_{n-1,k-1+i} \tag{1}$$

ということになる．ここで，$T_{0,0} = 1$，また $n > 0$ に対して $T_{n,0} = 0$

[1] ［訳註］簡単に見えないかも知れないが，2 行目以下をすべて第 1 行に足せば，すぐに対角行列に持ち込める．帰納法でやってもよい．ただし，行列のサイズが $n-1$ であることに注意する．サイズが m なら $(n-m)n^{m-1}$ になる．

とおいている．$T_{n,n}=1$ とするためには $T_{0,0}=1$ が必要である．

命題.

$$T_{n,k} \;=\; k\,n^{n-k-1} \qquad (2)$$

が成り立ち，とくに

$$T_{n,1} \;=\; T_n \;=\; n^{n-2}$$

となる．

■ **証明.** (1) から，帰納法を使って以下のように計算する．

$$\begin{aligned}
T_{n,k} &= \sum_{i=0}^{n-k}\binom{n-k}{i}(k-1+i)(n-1)^{n-1-k-i} \qquad (i \to n-k-i)\\
&= \sum_{i=0}^{n-k}\binom{n-k}{i}(n-1-i)(n-1)^{i-1}\\
&= \sum_{i=0}^{n-k}\binom{n-k}{i}(n-1)^{i} - \sum_{i=1}^{n-k}\binom{n-k}{i}i(n-1)^{i-1}\\
&= n^{n-k}-(n-k)\sum_{i=1}^{n-k}\binom{n-1-k}{i-1}(n-1)^{i-1}\\
&= n^{n-k}-(n-k)\sum_{i=0}^{n-1-k}\binom{n-1-k}{i}(n-1)^{i}\\
&= n^{n-k}-(n-k)n^{n-1-k} \;=\; k\,n^{n-1-k}.
\end{aligned}$$

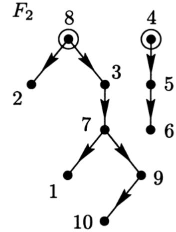
□

■ **第 4 の証明（2 重数え上げ）.** ジム・ピットマンによる次の驚くべきアイデアは，帰納法も全単射も使うことなく，ケイリーの公式とその一般化 (2) を与えるものであり，2 つの方法でうまく数えるだけである．

$\{1,\ldots,n\}$ 上の**根付きの森**とは，各成分の木に根を 1 つ選んだ森のことである．$\mathcal{F}_{n,k}$ を k 個の根付きの木からなる根付きの森の集合とする．すると，$\mathcal{F}_{n,1}$ はすべての根付きの木の集合になる．

$|\mathcal{F}_{n,1}|=nT_n$ に注意する．なぜなら，あらゆる木に対し，根の選び方は n 通りだからである．ここで，$F_{n,k}\in\mathcal{F}_{n,k}$ を，すべての辺を根から離れるように向きをつけた**有向**グラフと考える．森 F が別の森 F' を**含む**と言うのは，F が F' を有向グラフとして含むときとする．明らかに，

F が F' を真に含むなら，F の方が F' より成分の数は少なくなる．余白の図はそのような 2 つの森で，根は一番上としている．



F_2 は F_3 を含む．

決定的なアイデアを述べよう．森の列 $F_1, \ldots, F_k$ に対し，すべての i に対して $F_i \in \mathcal{F}_{n,i}$ でありかつ F_i が F_{i+1} を含むとき，この列を細分列であると呼ぶ．

ここで，F_k を $\mathcal{F}_{n,k}$ の中の固定した森とし，次の記号を考える．

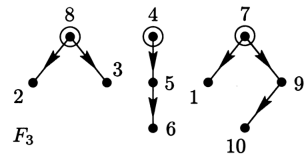
- $N(F_k)$ を，F_k を含む根付きの木の数とし，

- $N^*(F_k)$ を，F_k で終わる細分列の数とする．

$N^*(F_k)$ を，1 つは木から始め，もう 1 つは F_k から始めるという，2 つの方法で数えよう．$F_1 \in \mathcal{F}_{n,1}$ が F_k を含むと仮定する．F_1 から F_k への細分列を得るために，$F_1 \backslash F_k$ の $k-1$ 個の辺をどんな可能な順序で取り除いていってもよいので，

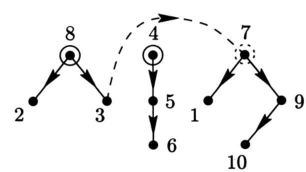
$$N^*(F_k) \;=\; N(F_k)\,(k-1)! \tag{3}$$

がわかる．



今度は反対側から始めよう．F_k から F_{k-1} を作るには，任意の頂点 a から，a を含まない木の $k-1$ 個の根の任意のものへ，有向辺を追加しなければならない（余白の図では，F_3 から F_2 へは，3 ●⟶● 7 という辺を付け加えている）．それで $n(k-1)$ 通りの選び方がある．同じように，F_{k-1} に対しては，任意の頂点 b から b を含まない木の $k-2$ 個の根へ，有向辺をつけてよい．このため，$n(k-2)$ 通りの選び方がある．これを続けると，

$$N^*(F_k) \;=\; n^{k-1}(k-1)! \tag{4}$$



$F_3 \longrightarrow F_2$

となり，これと (3) とから予期せぬ単純な関係式

$$N(F_k) = n^{k-1} \qquad (\text{任意の } F_k \in \mathcal{F}_{n,k} \text{に対して})$$

が得られることになる．$k = n$ のときは，F_n はちょうど n 個の孤立した頂点になる．それゆえ，$N(F_n)$ はすべての根付きの木の数を数えることになり，$|\mathcal{F}_{n,1}| = n^{n-1}$ が得られるので，ケイリーの公式も得られる． □

しかし，この証明からはこれ以上のことが得られる．公式 (4) からは，$k=n$ のとき，

$$\#\{\text{細分列 } (F_1, F_2, \ldots, F_n)\} = n^{n-1}(n-1)! \tag{5}$$

が得られる．$F_k \in \mathcal{F}_{n,k}$ に対して，$N^{**}(F_k)$ を，k 番目の項が F_k であるような細分列 $F_1, \ldots, F_n$ の数とする．明らかにこれは，$N^*(F_k)$ に $(F_{k+1}, \ldots, F_n)$ の選び方の数を掛けたものになる．しかし，この最後に述べた数は，F_k の $n-k$ 個の辺を可能な任意の方法で取り去ってもよいので，$(n-k)!$ となる．それで，

$$N^{**}(F_k) = N^*(F_k)(n-k)! = n^{k-1}(k-1)!(n-k)! \tag{6}$$

となる．この数は F_k の選び方によらないので，(5) を (6) で割れば，k 個の木を持つ根付きの森の数

$$|\mathcal{F}_{n,k}| = \frac{n^{n-1}(n-1)!}{n^{k-1}(k-1)!(n-k)!} = \binom{n}{k} k\, n^{n-1-k}$$

が得られる．k 個の根の選び方は $\binom{n}{k}$ 通りなので，帰納法に頼らなくても，公式 $T_{n,k} = kn^{n-k-1}$ を再証明できたことになる．

歴史的なコメントをして終わりにしよう．1889 年のケイリーの論文にはカール・W・ボルチャルト (1860) の先行論文があり，ケイリー自身もその事実を知っていた．同値な結果ならそれよりも前にジェームズ・J・シルヴェスター (1857) の論文にも出ている（[2, 第 3 章] 参照）．ケイリーの論文の新しさはグラフ理論の用語を使ったことであり，以来この定理は彼の名前と結びつけられてきた．

参考文献

[1] M. アイグナー：『組合せ論』(*Combinatorial Theory*), Springer-Verlag, Berlin Heidelberg New York 1979; Reprint 1997.

[2] N. L. ビッグス，E. K. ロイド，R. J. ウィルソン：『グラフ理論 1736-1936』(*Graph Theory 1736-1936*), Clarendon Press, Oxford 1976.

[3] A. ケイリー：「木についての定理」(*A theorem on trees*), Quart. J. Pure Appl. Math. **23** (1889), 376-378; Collected Mathematical Papers Vol. 13, Cambridge University Press 1897, 26-28.

[4] A. ジョイヤル：「形式的級数の組合せ論」(*Une théorie combinatoire des séries formelles*), Advances in Math. **42** (1981), 1-82.

[5] J. ピットマン：『ランダムな複合森』(*Coalescent random forests*), J. Combinatorial Theory, Ser. A **85** (1999), 165-193.

[6] H. プリューファー：「置換に関する 1 定理の新しい証明」(*Neuer Beweis eines Satzes über Permutationen*), Archiv der Math. u. Physik (3) **27** (1918), 142-144.

[7] A. レニイ：「木の理論におけるいくつかの注意」(*Some remarks on the theory of trees*). MTA Mat. Kut. Inst. Kozl. (Publ. math. Inst. Hungar. Acad. Sci.) **4** (1959), 73-85; Selected Papers Vol. 2, Akadémiai Kiadó, Budapest 1976, 363-374.

[8] J. リオーダン：「ラベル付きの木の森」(*Forests of labeled trees*), J. Combinatorial Theory **5** (1968), 90-103.

第25章　ラテン方陣を完成する

古い時代まで研究が遡ることのできることが明らかな，古い組合せ論の対象に**ラテン方陣**がある．ラテン方陣を得るには，$(n \times n)$ の正方形の形に並んだ n^2 の箱に，数 $1, 2, \dots, n$ を埋めて，あらゆる数があらゆる行とあらゆる列に一度だけ現れるようにしなければならない．言い換えれば，行と列はそれぞれ集合 $\{1, \dots, n\}$ の置換を表している．n をラテン方陣の**位数**と呼ぼう．

1	2	3	4
2	1	4	3
4	3	1	2
3	4	2	1

位数 4 のラテン方陣.

論じたいと思っている問題はこうである．誰かが箱に数 $\{1, 2, \dots, n\}$ を入れ始めたとする．あるとき入れるのを止めて，ラテン方陣ができるように残りの箱に数を入れてくれと，我々に頼んだとする．どんなときなら，できるだろうか？ ともかく可能性があるには，もちろん，引き受ける時点で，どんな元もあらゆる行と列に高々一度しか出てきていないと仮定しなければならない．この状況に名前をつけよう．$(n \times n)$ 配列のいくつかの箱に，集合 $\{1, \dots, n\}$ の数が入っていて，あらゆる数はあらゆる行と列に高々一度しか現れていないとき，位数 n の**部分ラテン方陣**と呼ぶ．すると問題は，

> **部分ラテン方陣から，いつ，同じ位数のラテン方陣を完成させることができるか？**

となる．

少し例を見てみよう．最初の $n-1$ 行に数が入っていて，最後の行が空だとしよう．このとき，最後の行に数を入れるのは簡単である．あらゆる元はこの部分ラテン方陣に $n-1$ 回現れているので，どれか 1 つの列の中には現れてこないことに注意する．それゆえ，各元をそれが出てこない列の底に書き込めば，正しく方陣が完成する．

1	4	2	5	3
4	2	5	3	1
2	5	3	1	4
5	3	1	4	2
3	1	4	2	5

巡回ラテン方陣.

正反対の場合として，最初の行だけが埋まっていると仮定する．そのときもまたラテン方陣を完成するのは簡単で，次の行に移るごとに元を巡回的に回転させればよい．

このように，第 1 の例にはラテン方陣の作り方は決まってしまっていたが，第 2 の例ではたくさんの可能性がある．一般に，あらかじめ埋まっている箱が少ないほど，ラテン方陣の作り方の自由度は大きくなる．

しかし，余白の例の部分ラテン方陣では n 個の箱しか埋まっていないが，ラテン方陣にすることはできない．というのは，行と列の条件を破らないで右上隅を埋める方法がないからである．

1	2	. . .	n-1	
				n

ラテン方陣にできない部分ラテン方陣.

もし $n \times n$ の配列で，埋まっている箱の数が n より少なければ，いつでもラテン方陣にすることができるか？

この問題は 1960 年にトレヴォー・エヴァンスによって提出され，ラテン方陣を完成させることが常に可能であるという主張は直ちにエヴァンス予想として知られるようになった．もちろん，帰納法でやってみることはできるし，結局はそれが成功への道である．しかし，1981 年のボーダン・スメタニウクの証明は問題の答えではあるが，そのようなことをするために帰納法の証明が必要とされる機微を示す美しい例になっている．そしてその上，この証明は構成的で，どんな部分配置からでも具体的にラテン方陣を完成することができるのである．

1	3	2
2	1	3
3	2	1

R: 1 1 1 2 2 2 3 3 3
C: 1 2 3 1 2 3 1 2 3
E: 1 3 2 2 1 3 3 2 1

この証明に進む前に，一般のラテン方陣を少し詳しく見てみることにする．ラテン方陣を，それと同値な $(3 \times n^2)$ な配列と見ることができ，それをラテン方陣の**線配列**と呼ぶ．余白の図は位数 3 のラテン方陣と対応する線配列を示している．R, C, E はそれぞれ行 (row)，列 (column)，元 (element) を表わしている[1]．

ラテン方陣に関する条件は，線配列のどの 2 つの線でもすべての n^2 個の順序対が現れ（したがってあらゆる対がちょうど 1 回現れ）るということと同値である．明らかに，各行のシンボルを（行，列，元の置換に対応して）任意に置換してよく，そうしてもラテン方陣が得られる．しかし，$(3 \times n^2)$ 配列に関する条件にはそれ以上の意味はない，つまり，

[1] ［訳註］R, C, E の i 番目の元を r_i, c_i, e_i とするとき，この線配列はラテン方陣の第 r_i 行，第 c_i 列に，e_i という数が入っていることを示している．

元が特別な役割を果たすことはないのである．配列の線を（全体として）置換することもできて，それも線配列に関する条件は保たれるのだから，ラテン方陣が得られるのである．

そのような置換によって結ばれるラテン方陣は**共役**であると言う．ここで，証明を見通しよくしてくれる事柄を見ておこう．部分ラテン方陣は明らかに，部分線配列（で，あらゆる対が，どの 2 つの線にも，高々1 回しか現れないようなもの）に対応しており，どんな部分ラテン方陣の共役もまた部分ラテン方陣になる．とくに，部分ラテン方陣がラテン方陣に拡張できることと任意の共役が拡張できることとは同値である（共役な部分ラテン方陣を拡張してから 3 本の線の置換を元に戻せばよい）．

上記の例の線を巡回的に $R \longrightarrow C \longrightarrow E \longrightarrow R$ と置換すれば，次の線配列とラテン方陣が得られる．

1	2	3
3	1	2
2	3	1

R : 1 3 2 2 1 3 3 2 1
C: 1 1 1 2 2 2 3 3 3
E: 1 2 3 1 2 3 1 2 3

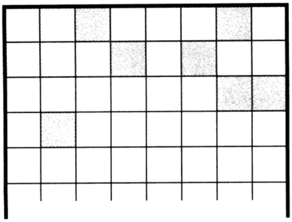
スメタニウクの定理より先に知られていた，ライザーとリンドナーによる 2 つの結果が必要となる．部分ラテン方陣が，最初の r 行が完全に埋まっていて残りの箱が空であるときに，$(r \times n)$ **ラテン長方形**と言おう．

補題 1. どんな $(r \times n)$ ラテン長方形も，$r < n$ のとき，$(r+1) \times n$ ラテン長方形に拡張することができ，それゆえラテン方陣に拡張できる．

■ **証明.** ホールの定理（第 22 章参照）を使う．A_j を第 j 列に現れない数の集合とする．許される第 $(r+1)$ 行は，まさに，集合族 $A_1, \ldots, A_n$ に対する異なる元による代表系に対応している．したがって，補題を証明するにはホールの条件 (H) を確かめないといけない．あらゆる集合 A_j の大きさは $n-r$ であり，あらゆる元はちょうど $n-r$ 個の集合 A_j に属している（長方形の中には r 回現れているからである）．集合 A_j たちから m 個とれば，合わせて $m(n-r)$ 個の元を含むので，少なくとも m 個は異なっている．これが条件 (H) である． □

補題 2. P を位数 n の部分ラテン方陣で，高々 $n-1$ 個の箱に，高々 $\frac{n}{2}$ 個の異なる元が埋まっているものとすると，P は位数 n のラテン方陣に拡張することができる．

■ **証明.** 最初に問題を少し扱いやすい形に変える．上で述べた共役の原理によって，「高々 $\frac{n}{2}$ 個の異なる元」という条件を「高々 $\frac{n}{2}$ の行にだけ元が入っている」という条件に置き換えてもよく，さらにこれらの行が上から詰まっていると仮定してもよい．つまり，箱に数が入っているのは第 $1, 2, \ldots, r$ 行で，第 i 行では f_i 個の箱に数が入っていて，$r \leq \frac{n}{2}$ かつ $\sum_{i=1}^{r} f_i \leq n-1$ であるとする．そこで行を入れ換えて，



最初の状況では $n=8$, $\ell=3$, $f_1=f_2=f_3=2$, $f_4=1$ である．濃い影の箱はあらかじめ埋まっていた箱を表わし，薄い影の箱は拡張して行く中で埋められた箱を表している．

$f_1 \geq f_2 \geq \cdots \geq f_r$ であるとしてよい．今度は，第 $1,2,\ldots,r$ 行を少しずつ埋めていき，それを，補題 1 によってラテン方陣に拡張できることがわかっている $(r \times n)$ 長方形になるまで行う，

すでに第 $1,2,\ldots,\ell-1$ 行が埋められていて，第 ℓ 行で埋まっているのは f_ℓ 個の箱で，それらは後ろの方に詰まっていると仮定する．この状況は図に描いたようになっている． ここで，影のついている箱には数が入っている．

第 ℓ 行に数を入れるためには，ホールの定理をもう一度使うのだが，今回はもっと微妙な使い方をする．X を第 ℓ 行に出てきていない元の集合とすると，$|X|=n-f_\ell$ であり，$j=1,\ldots,n-f_\ell$ に対して，A_j を第 j 列に出てきていない X の元（第 ℓ 行の上にも下にも出てきていないことになる）の集合とする．それゆえ，第 ℓ 行を埋めつくすために，集合族 $A_1,\ldots,A_{n-f_\ell}$ に対して条件 (H) を確かめなくてはいけない．

最初に，

$$n-f_\ell-\ell+1 \quad > \quad \ell-1+f_{\ell+1}+\cdots+f_r \tag{1}$$

となることを示す．$\ell=1$ の場合は明らかである．そうでない場合は，$\sum_{i=1}^r f_i < n$, $f_1 \geq \cdots \geq f_r$, $1<\ell \leq r$ を合わせると，

$$n \quad > \quad \sum_{i=1}^r f_i \quad \geq \quad (\ell-1)f_{\ell-1}+f_\ell+\cdots+f_r$$

が得られる．すると，$f_{\ell-1} \geq 2$ となるか（このときは (1) が成り立つ），$f_{\ell-1}=1$ となるかである．あとの場合，(1) は $n > 2(\ell-1)+r-\ell+1 = r+\ell-1$ となるが，これは $\ell \leq r \leq \frac{n}{2}$ なので成り立つ．

さて，$1 \leq m \leq n-f_\ell$ とし，集合 A_j を m 個とって，その和集合を B とする．$|B| \geq m$ を示さねばならない．A_j たちに対応する m 個の列の中で，X の元を含む箱の数 c を考える．

そのような箱の数は，第 ℓ 行の上方には高々 $(\ell-1)m$ であり，下方には高々 $f_{\ell+1}+\cdots+f_r$ なので，

$$c \quad \leq \quad (\ell-1)m+f_{\ell+1}+\cdots+f_r$$

となる．一方，各元 $x \in X \backslash B$ は m 個の列のそれぞれに現れるので，$c \geq m(|X|-|B|)$ であり，したがって（$|X|=n-f_\ell$ に注意して）

$$|B| \quad \geq \quad |X| - \tfrac{1}{m}c \quad \geq \quad n - f_\ell - (\ell - 1) - \tfrac{1}{m}(f_{\ell+1} + \cdots + f_r)$$

となる．これから，

$$n - f_\ell - (\ell - 1) - \tfrac{1}{m}(f_{\ell+1} + \cdots + f_r) \quad > \quad m - 1$$

であれば，つまり

$$m(n - f_\ell - \ell + 2 - m) \quad > \quad f_{\ell+1} + \cdots + f_r \qquad (2)$$

であれば，$|B| \geq m$ となることになる．

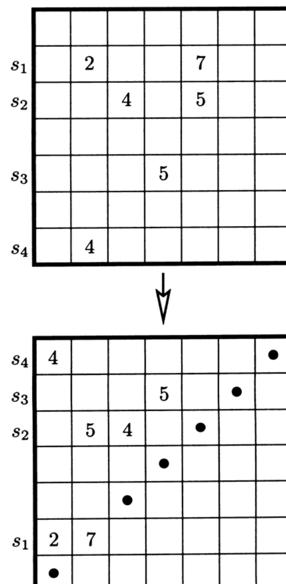
不等式 (2) は，$m = 1$ のときと $m = n - f_\ell - \ell + 1$ のときは，(1) によって正しいし，それゆえ 1 と $n - f_\ell - \ell + 1$ の間のすべての値 m に対しても正しい．なぜなら，左辺は m に関する 2 次関数で，最高次の係数が -1 だからである．残っているのは $m > n - f_\ell - \ell + 1$ の場合である．X のどんな元 x も高々 $\ell - 1 + f_{\ell+1} + \cdots + f_r$ 個の行にしか含まれないので，また高々同じ数の列にしか現れない．もう一度 (1) に訴えると，x が集合 A_j の 1 つに属すことがわかるので，この場合，$B = X$ であり，$|B| = n - f_\ell \geq m$ と結論され，証明が終わる． □

最後にスメタニウクの定理を証明しよう．

定理． **高々 $n-1$ 個の箱しか埋まっていない位数 n の部分ラテン方陣から，同じ位数のラテン方陣に拡張することができる．**

■ **証明．** n に関する帰納法を使う．$n \leq 2$ の場合は自明である．P が位数 $n+1$ の部分ラテン方陣で，高々 n 個の箱しか埋まっていないとする．補題 2 により，互いに異なっている元が $\frac{n+1}{2}$ 個より多いと仮定してよく，それゆえ一度しか現れていない元が存在する．それを $n+1$ としよう．前と同じように，r 個の，部分的に，それぞれ $f_1, \ldots, f_r$ 個の箱が埋まっている行 $s_1, \ldots, s_r$ があるとしよう．$\sum_{i=1}^{r} f_i \leq n$ となっている．さらに，$n+1$ が埋まっているのが第 s_1 行であると仮定する．

第 1 段階として，埋まっている箱をすべて逆対角線より上に動かし，ただ $n+1$ が埋まっている箱だけは逆対角線上にくるようにする．（逆対角線は $i + j = n + 2$ を満たす箱 (i, j) からなっている．）これは以下のようにして行う．第 s_1 行を $n + 2 - f_1$ 番目の行へ動かす．列を置換することによって，埋まっている箱を左に動かし，$n+1$ がこの行の最後にくるように，それゆえ逆対角線上にくるようにする．次に，第 s_2 行



を $n+1-f_1-f_2$ 番目の行に動かし，埋まっている箱をできるだけ左に動かす．一般に，第 s_i 行を $n+1-f_1-f_2-\cdots-f_i$ 番目の行に動かし，埋まっている箱をできるだけ左に動かす．こうすれば明らかに欲しかった状態にできる．前ページの余白の上の方の図は $n+1=7$ の場合の例を示している．

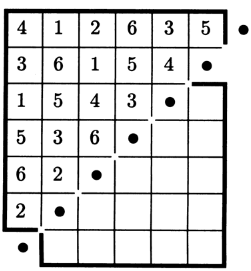
L

4	1	2	6	3	5
3	6	1	**5**	4	2
1	**5**	**4**	3	2	6
5	3	6	2	1	4
6	2	3	4	5	1
2	4	5	1	6	3

ここが証明のアイデアの主要部分である．元 $n+1$ と，最後の行と列を取り除く．帰納法により，残された位数 n の部分ラテン方陣は位数 n のラテン方陣 L に拡張することができる．左の余白にあるのは，前ページの余白の上の部分ラテン方陣の（多くの）拡張のうちの 1 つである．

次に，ラテン方陣 L を 2 つに切り離し，逆対角線を含んで上側の箱はそのままにし，下側の箱は空にして，1 箱分下に下げる．こうして半分埋まった長方形 L' が得られる．上の例に対してのものは余白に図示してある．

L'



注意しておくが，L' のあらかじめ与えられていたすべての箱（元 $n+1$ を除いて）は逆対角線の上方の「上半分」の中に入っている．それゆえ，もし L' の下半分を数 $1,\ldots,n$ で埋めて（今度は位数 $n+1$ の）部分ラテン方陣になるようにできれば，逆対角線上を $n+1$ で埋め，一意的な最終列を付け加えれば（補題 1 の自明な場合にあたる），証明は完成する．この最終段階を実行するのに，ラテン方陣 L の情報を参考にしながら，下半分の行を 1 行ずつ埋めて行くようにする．

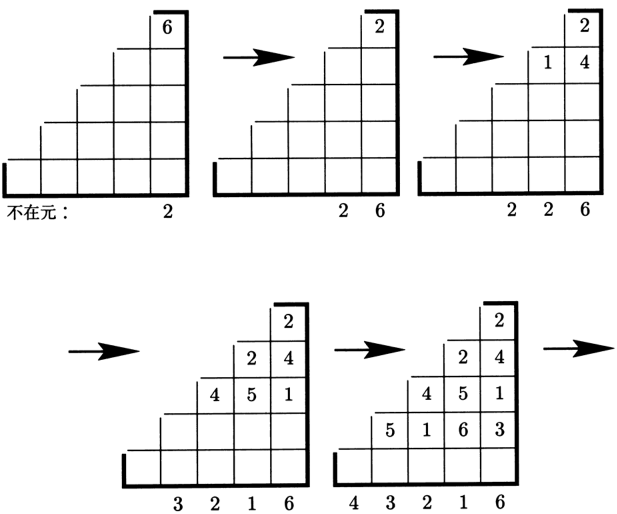
$k\geq 3$ とし，帰納的に，以下の条件を満たすように第 $3,\ldots,k-1$ 行が埋められたと仮定する．

- $n-k+3\leq j\leq n$ に対して，L' の第 j 列の $n+1$ 以外の $k-2$ 個の元は，もとのラテン方陣 L の第 j 列の最初の $k-1$ 個の成分の中にある．各列にちょうど 1 つの「不在元」が存在する．
- L' の各列の不在元 x_j は互いに異なる．

そこで第 k 行に移ろう．$y_{n-k+2},\ldots,y_n$ を，ラテン方陣 L の第 k 行の逆対角線を含んで右側の元であるとする．つまり，y_{n-k+2} が第 $n-k+2$ 列の新しい不在元である．まずは，第 k 行を元 $y_{n-k+3},\ldots,y_n$ で埋めてみることにしよう．注意しておくが，第 k 行の全体は許される並びになっていて，すべての j に対して，$x_j\neq y_j$ となっている．それはこれらの元が L の同じ列 j からきた元だからである．だから，これでよいのだが，ある $j\geq n-k+3$ に対して $y_{n-k+2}=x_j$ となると困る．な

ぜなら，そのときは不在元の条件が壊れてしまうからである．その場合には，x_j と y_j を交換する．新しい第 k 行も許される並びである（というのは，$x_j = y_{n-k+2}$ であり，y_{n-k+2} はそれまでに第 k 行にいたからである）．だから，ある $\ell \neq j$ に対して $y_j = x_\ell$ とならないのなら，これで終わりである．そうなるときには，x_ℓ と y_ℓ を交換し，また同じようにして行く．明らかに，このプロセスは欲しかった結果になれば終わりなわけで，最後までやるとしてもすべての x_i が第 k 行に移されるまでのことである．このようにして，第 n 行までのすべての行を埋めてしまう．最後の第 $n+1$ 行は不在元で埋めてしまうことができ，証明が終わる． □

次の図は，この埋めて行く過程を，上の例の場合に示したものである．



4	1	2	6	3	5	**7**
3	6	1	5	4	**7**	2
1	5	4	3	**7**	2	6
5	3	6	**7**	2	4	1
6	2	**7**	4	5	1	3
2	**7**	5	1	6	3	4
7	4	3	2	1	6	5

参考文献

[1] T. エヴァンス：「不完全なラテン方陣の埋め込み」(*Embedding incomplete Latin squares*), Amer. Math. Monthly **67** (1960), 958-961.

[2] C. C. リンドナー：「ラテン長方形を完全にすることについて」(*On completing Latin rectangles*), Canadian Math. Bulletin **13** (1970), 65-68.

[3] H. J. ライザー：「組合せ論的定理とラテン方陣への応用」(*A combinatorial theorem with an application to Latin rectangles*), Proc. Amer. Math. Soc. **2** (1951), 550-552.

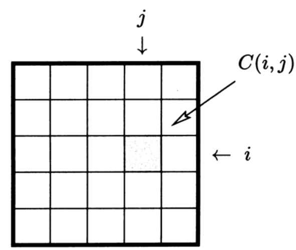
[4] B. スメタニウク：「ラテン方陣の新しい構成 I：エヴァンス予想の証明」(*A new construction on Latin squares I: A proof of the Evans conjecture*), Ars Combinatoria **11** (1981), 155-172.

第26章　ディニッツの問題

4 色問題がグラフ理論の発展に対する主な推進力であったことは今では知られていることだが，彩色はいまだに多くのグラフ理論家が一番好む話題である．ここで単純に見える彩色問題を考えるが，これは 1978 年にジェフ・ディニッツによって提出され，15 年後にフレッド・ギャルヴィンによって驚くほど単純な解答が与えられるまで，すべての攻撃を退(しりぞ)けてきたものである．

n^2 個の箱が大きさ $(n \times n)$ の正方形の形に並べられ，第 i 行第 j 列の箱を (i, j) と書くことにする．各箱 (i, j) に対して n 個の色の集合 $C(i, j)$ が与えられているとする．

そのとき，それぞれの箱 (i, j) から集合 $C(i, j)$ の中の色を拾い出して，各行各列の色がすべて互いに異なるように，正方形全体を常に彩色することができるか？



初めに，色の集合 $C(i, j)$ がすべて同じで，たとえば $\{1, 2, \ldots, n\}$ であるという場合を考える．そのとき，ディニッツの問題は「$(n \times n)$ 正方形に数 $1, 2, \ldots, n$ を入れて，どの行もまたどの列も異なる数からなるようにする」ことに帰着する．言い換えれば，そのような彩色は，前章で議論したラテン方陣に対応している．だから，この場合，問題の答えは「できる」である．

これがあまりに簡単だから，集合 $C = \bigcup_{i,j} C(i, j)$ が n より多い色を含むという一般の場合にそんなに難しくなる筈はないように見える．困難さはむしろ，C のあらゆる色がそれぞれの箱で使うことができないと

$\{1,2\}$	$\{2,3\}$
$\{1,3\}$	$\{2,3\}$

いう事実からくるのである．たとえば，ラテン方陣の場合は明らかに第 1 行に対して色の集合の任意の置換を選ぶことができるのに，一般の問題ではそうはなっていないのである．$n = 2$ の場合ですでに，この難点の説明ができる．

図に示したように色の集合が与えられているとする．第 1 行で色の 1 と 2 を選んだとすれば，面倒なことになる．第 2 行の 2 つの箱の色として 3 を選ばなければならないからである．

ディニッツの問題に取り組む前に，状況をグラフ理論の言葉で言い直してみる．いつものように，ループと多重辺を持たないグラフ $G = (V, E)$ だけを考える．$\chi(G)$ をグラフの**彩色数**とする．つまり，隣り合う頂点では違う色になるように，頂点に与える色の最小数とする．

言い換えれば，彩色とは，(同じ色で彩色された）類への V の分割で，1 つの類の中には辺が存在しない[1]ようなもののことである．集合 $A \subseteq V$ が**独立**であるというのを A の中に辺がないこととすると，彩色数とは，頂点集合 V を分割する独立な集合の最小数であることになる．

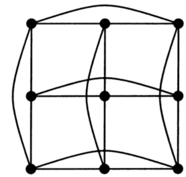
1976 年にヴィジングが，そしてその 3 年後にエルデシュ，ルービン，テイラーの 3 人が，ディニッツの問題に直接導かれるような，彩色問題を次のように変形した問題を研究した．グラフ $G = (V, E)$ において，各頂点 v に対して色の集合 $C(v)$ が与えられているとする．**リスト彩色**とは，各 $v \in V$ に対して $c(v) \in C(v)$ であるような彩色 $c : V \longrightarrow \bigcup_{v \in V} C(v)$ のことである．すると，**リスト彩色数** $\chi_\ell(G)$ の定義は明らかであって，すべての $v \in V$ に対して $|C(v)| = k$ を満たす色の集合 $C(v)$ のどんなリストに対しても常にリスト彩色が存在するような最小の数 k のことである．もちろん $\chi_\ell(G) \leq |V|$ である（色が足りなくなることはないから）．通常の彩色はすべての集合 $C(v)$ が同じであるときのリスト彩色の特殊な場合に過ぎないので，どんなグラフ G に対しても

$$\chi(G) \quad \leq \quad \chi_\ell(G)$$

1　［訳註］誤解を生み勝ちな表現だが，以下でもよく出てくるのでここで注意しておく．類は頂点の集合で，その中には元々辺などないが，ここで言っているのは，そのような集合に属す任意の頂点を結ぶ辺が G の中にないということである．言葉の誤用と言うべきだが，一々言わなくても了解されるような場合に状況説明を省略するということである．専門家にありがちなことだが，グラフ理論に慣れていないと戸惑うことがあるかも知れない．

となる．

ディニッツの問題に戻って，頂点集合が $(n \times n)$ 配列の n^2 個の箱であり，2 つの箱が辺で結ばれるのを同じ行か同じ列になるときとするようなグラフ S_n を考える．



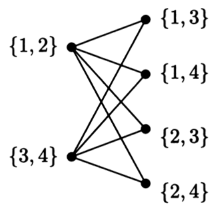
グラフ S_3.

1 つの行にあるどんな n 個の箱も互いに隣り合っている（辺で結ばれている）ので，少なくとも n 色は必要である．さらに，n 色での彩色はどれも，色のクラスをなすのと同じ数によって埋められた箱を持つラテン方陣に対応する．すでに知っているようにラテン方陣は存在するので，$\chi(S_n) = n$ となって，いまやディニッツの問題は

$$\chi_\ell(S_n) \ = \ n\,?$$

と簡潔に述べることができる．

どんなグラフ G に対しても $\chi(G) = \chi_\ell(G)$ になるだろうと考えるかも知れないが，これは真実からかけ離れたところにある．グラフ $G = K_{2,4}$ を考える．その彩色数は 2 である．というのは，左にある頂点には 1 つの色を右にある頂点にはもう 1 つの色を使ってもよいからである．しかしそこで，図にあるように色の集合が与えられたとしよう．



左の頂点の彩色には 4 つの可能性 1|3, 1|4, 2|3, 2|4 があるが，この対のうちのどの 1 つも右側の色の集合として出てきているので，リスト彩色は不可能である．それゆえ $\chi_\ell(G) \geq 3$ であるが，実際に $\chi_\ell(G) = 3$ となることの証明は読者の楽しみに残しておく（すべての可能性を確かめる必要はない！）．この例を一般化して，$\chi(G) = 2$ ではあるが，$\chi_\ell(G)$ が任意に大きいグラフを見つけることは難しくない！ だから，リスト彩色問題はちょっと見に思うほど易しくはない．

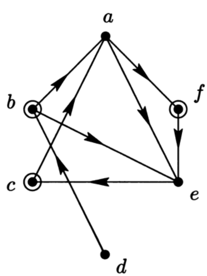
ディニッツの問題に戻ろう．解に向かって重要な歩を進めたのはジャネッテ・ジャンセンで，1992 年に彼女は $\chi_\ell(S_n) \leq n+1$ であることを証明した．**止めの一撃**は，それぞれ以前から知られていた 2 つの結果を天才的に結びつけたフレッド・ギャルヴィンによってもたらされた．この 2 つの結果を述べ，それから $\chi_\ell(S_n) = n$ がどのようにして得られるかを示そう．

まず記法を決めておこう．v をグラフ G の頂点とすると，$d(v)$ を前と同じように v の**次数**とする．上の正方形グラフ S_n では，あらゆる頂点の次数は $2n-2$ である．同じ行にも列にも他の頂点は $n-1$ 個ずつあるからである．部分集合 $A \subseteq V$ に対して，A を頂点集合とし，A の

頂点の間の G のすべての辺を含む部分グラフを G_A と書く．この G_A を A から誘導された部分グラフと言い，ある A に対して $H = G_A$ となる H を G の**誘導部分グラフ**と言う．

最終的な結果を述べるために，あらゆる辺 e が向き付けを持っている**有向グラフ** $\vec{G} = (V, E)$ が必要になる．始点が u で，終点が v の弧 e があることを，$e = (u, v)$ という記号，または $u \longrightarrow v$ で表わす．すると，**出次数** $d^+(v)$ とか**入次数** $d^-(v)$ ということに意味が出てくる．ここで，$d^+(v)$ は v を始点とする辺の数で，$d^-(v)$ は v を終点とする辺の数であり，$d^+(v) + d^-(v) = d(v)$ となっている．G と書くときは，グラフ $\vec{G}$ の向き付けを無視したものの意味である．

次の概念はゲームの解析に起源を持つもので，以下の議論で決定的な役割を果たしている．



定義 1. $\vec{G} = (V, E)$ **を有向グラフとする．**<u>**核**</u> $K \subseteq V$ **とは次の 2 つを満たす頂点集合の部分集合のことである．**

(i) K **は** G **の中で独立である（つまり，**K **の頂点同士を結ぶ辺はない）．**

(ii) あらゆる $u \notin K$ **に対して，**$v \in K$ **を終点とする辺** $u \longrightarrow v$ **が存在する．**

図の例を見ると，集合 $\{b, c, f\}$ は核をなすが，$\{a, c, e\}$ から誘導された部分グラフは核を持たない．というのは 3 辺からなるサイクルがそれらの頂点を通っているからである．

これらの準備のもとで，最初の結果が述べられるようになった．

補題 1. $\vec{G} = (V, E)$ **を有向グラフとし，あらゆる頂点** $v \in V$ **に対して，出次数より大きいサイズの色の集合** $C(v)$ **があるとする．つまり，**$|C(v)| \geq d^+(v) + 1$ **とする．もし** $\vec{G}$ **のあらゆる誘導部分グラフが核を持つなら，各** v **に対して** $C(v)$ **に属する色による** G **のリスト彩色が存在する．**

■ **証明．** $|V|$ に関する帰納法で行う．$|V| = 1$ のときは証明すべきことはない．色 $c \in C = \bigcup_{v \in V} C(v)$ を 1 つ選び，

$$A(c) = \{v \in V : c \in C(v)\}$$

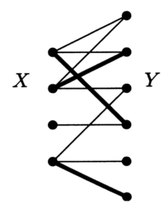
とおく．仮定により，誘導された部分グラフ $G_{A(c)}$ は核 $K(c)$ を持つ．

そこですべての $v \in K(c)$ に色 c を塗り（これは $K(c)$ が独立だから可能である），G から $K(c)$ を除き，C から c を除く．G' を $V\backslash K(c)$ 上の G の誘導部分グラフで，新しい色の集合のリストを $C'(v) = C(v)\backslash c$ とする．(核の条件 (ii) から）各 $v \in A(c)\backslash K(c)$ に対して出次数 $d^+(v)$ は少なくとも 1 は小さくなる．だから，$d^+(v)+1 \leq |C'(v)|$ は $\vec{G}'$ でも成り立っている．同じ条件が $A(c)$ の外側の頂点に対しても成り立っている．というのはこの場合，色の集合 $C(v)$ は変わらないままだからである．新しいグラフ G' の頂点の数は G より小さいので，帰納法によって証明は終わる． □

いまやディニッツの問題の攻撃法は明らかである．グラフ S_n の向き付けで，すべての v に対して出次数が $d^+(v) \leq n-1$ を満たし，すべての誘導部分グラフに対する核の存在を保証してくれるようなものを見つけることである．このことは第 2 の結果によって行われる．

また少し準備が必要となる．(第 8 章を）思い出すと，**2 部**グラフ $G = (X \cup Y, E)$ とは次の性質を満たすグラフのことだった．頂点集合 V は 2 つの部分 X と Y に分かれ，あらゆる辺の端点が一方は X に他方は Y にある．言い換えれば，2 部グラフとはまさに 2 色で（X に対して 1 つの色，Y に対して 1 つの色）彩色することのできるグラフのことである．

さて，実生活的な解釈ができる「安定マッチング」という重要な概念がある．2 部グラフ $G = (X \cup Y, E)$ における**マッチング** M とは，M に属するどの 2 つの辺も共通の端点を持たないような辺の集合のことである．余白の図では，太線で描いた辺が 1 つのマッチングをなしている．



2 部グラフとマッチング.

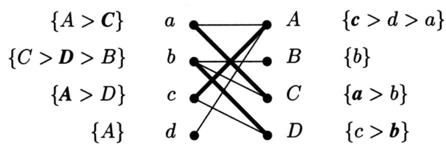
X を男性の集合，Y を女性の集合と考え，$uv \in E$ が u と v が結婚するかも知れないと解釈する．そのときマッチングは誰も重婚を犯さない集団結婚を意味している．現在の目的のためには，もっと細かい（そしてもっと現実的な？）マッチングの概念が必要で，これはゲイルとシャプリーによって提案された．明らかに，実際の生活では，人には好みというものがあり，このことを付け加えたものである．$G = (X \cup Y, E)$ において，あらゆる $v \in X \cup Y$ に対し，v に隣り合う頂点の集合 $N(v)$ にランク付けがある，つまり，$N(v) = \{z_1 > z_2 > \cdots > z_{d(v)}\}$ となっていて，z_1 が v にとっての一番の選択で，次が z_2 で，などとなっているのである．

定義 2. $G = (X \cup Y, E)$ のマッチング M は次の条件を満たすとき，安

定であると呼ぶ．$uv \in E \backslash M$, $u \in X$, $v \in Y$ であれば，$N(u)$ に属する $y > v$ があって $uy \in M$ となるか，$N(v)$ に属する $x > u$ があって $xv \in M$ となるか，またはその双方が成り立つかである．

実生活的な解釈では，結婚の集合が安定なのは，u と v が結婚しておらず，u が（妻があったとして）妻より v を好きであり，かつ v が（夫があったとして）夫より u を好きであるということが決して起こらないときである．そんなことが起こったら，まったくもって，状況はとても不安定になるだろう．

第 2 の結果を証明する前に，次の例を見てみよう．



太線の辺は安定な結婚を構成しており，優先順位のリストで安定な結婚に導く選択が太字で書かれている．

この例では，4 つの辺を持つ最大のマッチング M は一意的で $M = \{aC, bB, cD, dA\}$ となるが，M は安定ではない（cA を考えよ）ことに注意しよう．

補題 2．安定なマッチングは常に存在する．

■ **証明．** 次のアルゴリズムを考える．最初の段階では，すべての男性 $u \in X$ は，一番目に選んだ女性にプロポーズする．もし女性が 2 つ以上のプロポーズを受けたのなら，そのうち一番の人を選んで婚約し，プロポーズが 1 つだけならその人と婚約する．残りの男性は拒否されたのでリザーブの集合 R をなす．第 2 の段階では，R に属すすべての男性は次に選んだ女性にプロポーズする．女性はプロポーズを（もしいれば婚約者とも）比較して一番好きな男性を選んで婚約する．残りの男性は拒絶され，新しい集合 R をなす．そこで R に属すすべての男性は次に選んだ女性にプロポーズし，とこれを次々に行って行く．一番最後に選んだ女性にプロポーズしても断られた男性は以降の考察から（リザーブの集合からも）はずす．明らかにいつかはリザーブの集合 R は空になり，この時点でアルゴリズムは終了する．

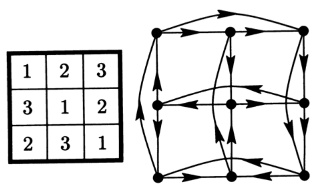
主張. アルゴリズムが終わったとき，婚約している男性と対応する女性とは安定なマッチングをなしている.

最初に注意しておくことは，ある特定の女性と婚約している男性は（その女性の）好みが増えるように変わっていくことである．というのも，各段階で，女性は新しいプロポーズと現在の相手とを比較して，新しく一番の男性を選ぶからである．それゆえ，$uv \in E$ だが $uv \notin M$ であるなら，u は v にはプロポーズをしていないか（その場合は，彼は v にまで廻る前によりよい相手を見つけたわけで，$N(u)$ に属するある $y > v$ に対して $uy \in M$ となっている），または u は v にプロポーズはしたが断られたことになる（そのときは，$N(v)$ に属する $x > u$ に対して $xv \in M$ となっている）．しかし，このことは安定なマッチングの条件そのものである． □

さて，補題1と補題2を合わせると，ディニッツの問題に対するギャルヴィンの解が得られる．

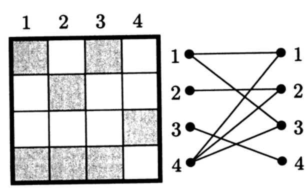
定理. すべての n に対して，$\chi_\ell(S_n) = n$ が成り立つ．

■ **証明.** 前と同じように，S_n の頂点を $(i,j), 1 \le i,j \le n$ と書く．(i,j) と (r,s) が辺で結ばれるのは，$i = r$ または $j = s$ が成り立つときかつそのときに限る．数字 $\{1,2,\ldots,n\}$ を埋めたラテン方陣を任意にとり，箱 (i,j) の中身を $L(i,j)$ と書く．次に向き付けを定めて S_n を有向グラフ $\vec{S}_n$ にする．水平な辺に対しては，$L(i,j) < L(i,j')$ のときに $(i,j) \longrightarrow (i,j')$ とし，垂直な辺に対しては，$L(i,j) > L(i',j)$ のときに $(i,j) \longrightarrow (i',j)$ とする．つまり，水平には小さな元から大きな元に向きを付け，垂直にはその反対にするのである.（余白には $n=3$ のときの例がある.）

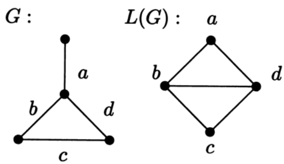


すべての (i,j) に対して $d^+(i,j) = n-1$ となることに注意する．実際，$L(i,j) = k$ であれば，第 i 行の $n-k$ 個の箱には k より大きな数が入っており，第 j 列の $k-1$ 個の箱には k より小さな数が入っている．

補題1から，あとは $\vec{S}_n$ のあらゆる誘導部分グラフが核を持つことを示せばよい．部分集合 $A \subseteq V$ を考え，X を L の行の集合，Y を列の集合とする．A に対して2部グラフ $G = (X \cup Y, A)$ を次のようにして対応させる．あらゆる $(i,j) \in A$ は $i \in X, j \in Y$ を結ぶ辺 ij を表わしていると考える．余白の例では A の箱には影をつけてある．



S_n 上の向き付けから，自然に $G=(X\cup Y,A)$ の近傍のランク付けが定まる．$\vec{S}_n$ で $(i,j)\longrightarrow(i,j')$ のときに，$N(i)$ では $j'>j$ とし，$(i,j)\longrightarrow(i',j)$ のときに，$i'>i$ とする．補題2によって，$G=(X\cup Y,A)$ は安定なマッチング M を持つ．この M が，A の部分集合として，欲しかった核になっている！ それがなぜかを見るために，まず M が A で独立であることに注意する．これは，$G=(X\cup Y,A)$ の辺と見るとき，端点 i または j を共有しないからである．次に，$(i,j)\in A\backslash M$ であれば，安定なマッチングの定義から，$j'>j$ であるような $(i,j')\in M$ が存在するか，$i'>i$ を満たすような $(i',j)\in M$ が存在するかとなる．このことは $\vec{S}_n$ で考えると $(i,j)\longrightarrow(i,j')\in M$ か $(i,j)\longrightarrow(i',j)\in M$ かになることを意味しており，証明が完結する．　□



線グラフの構成.

話を終えるためにもう少し進もう．読者は，グラフ S_n がある2部グラフから簡単に構成されることに気づいているかもしれない．$|X|=|Y|=n$ で，X と Y との間のすべての対を辺としている完全2部グラフ $K_{n,n}$ を考える．$K_{n,n}$ の辺をある新しいグラフの頂点と考え，そのような頂点を結ぶのを $K_{n,n}$ の辺として見たとき共通の端点を持つときとすれば，明らかに正方形グラフ S_n が得られる．S_n を $K_{n,n}$ の**線グラフ**と呼ぼう．さて．この構成はどんなグラフ G に対しても行うことができ，得られるグラフは G の**線グラフ** $L(G)$ と呼ばれる．

一般に，あるグラフ G に対して $H=L(G)$ となっているとき，H を**線グラフ**と呼ぶ．もちろん，あらゆるグラフが線グラフになれるわけではない．前に考察したグラフ $K_{2,4}$ はその例になっており，このグラフに対しては $\chi(K_{2,4})<\chi_\ell(K_{2,4})$ であることを知っている．しかし，H が線グラフであったら，どうだろうか？ 上の定理の証明を手直しして，H がある **2部**グラフの線グラフであるなら $\chi(H)=\chi_\ell(H)$ が成り立つことを，容易に示すことができる．そしてその方法によって，この分野で最高の予想

あらゆる線グラフ H に対し，$\chi(H)=\chi_\ell(H)$ となるか？

を確かめるという方向に何らかの前進があるかも知れない．この予想についてはごく僅かなことしか知られておらず，困難なように見える．だが，それを言えば，ディニッツの問題も20年前にはそうだったのだ．

参考文献

[1] P. エルデシュ, A. L. ルービン, H. テイラー：「グラフにおける選択可能性」(*Choosability in graphs*), Proc. West Coast Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium **26** (1979), 125-157.

[2] D. ゲイル, L. S. シャプリー：「カレッジの入学と結婚の安定性」(*College admissions and the stability of marriage*), Amer. Math. Monthly **69** (1962), 9-15.

[3] F. ギャルヴィン：「2部多重グラフのリスト彩色指数」(*The list chromatic index of a bipartite multigraph*), J. Combinatorial Theory, Ser. B **63** (1995), 153-158.

[4] J. C. M. ジャンセン：「長方形に対して解かれたディニッツの問題」(*The Dinitz problem solved for rectangles*), Bulletin Amer. Math. Soc. **29** (1993), 243-249.

[5] V. G. ヴィジング：「グラフの頂点を定めた色で彩色すること」(*Coloring the vertices of a graph in prescribed colours*)（ロシア語）, Методы Дискрет. Анализ. **101** (1976), 3-10.

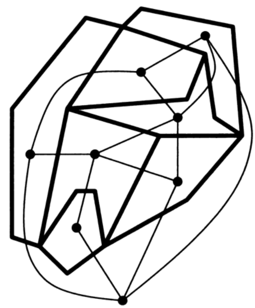
グラフ理論



「4 色地理学者」

第27章　5色平面グラフ

4色問題との関連から，平面グラフとその彩色は，グラフ理論が始まって以来，集中的に研究されてきたテーマであった．元々の言い方では，4色問題は，平面上の地図の領域を4色で，しかも境界を共有する（1点だけのときは除いて）領域には異なる色になるように彩色することが，いつでも可能かどうかを問うものであった．右の図が示しているように，地図の領域の彩色は，平面グラフの頂点の彩色と全く同じことをすることになる．第10章（83ページ）でしたように，各領域（と外側の領域）の内部に頂点を置き，隣り合う領域に属すそのような2頂点を共通の境界を通る辺で結ぶ．



地図の双対グラフ．

そのとき，得られたグラフ G は，地図 M の**双対グラフ**というが，平面グラフになり，普通の意味での G の頂点の彩色は M の領域の彩色と同じものである．だから，平面グラフの頂点彩色に集中してもよく，以降はそうすることにする．G がループや多重辺を持たないと仮定してよいことに注意する．というのは，そういうものは彩色に対しては意味がないからである[1]．

4色定理を証明する攻撃の長く困難な歴史の中で，多くの試みがもう少しのところまで行っていたが，最終的に1976年のアッペルとハーケ

---

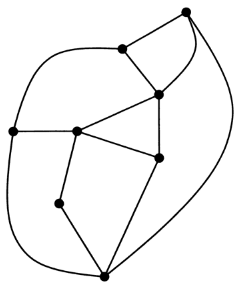
[1] ［訳註］多重辺は，1組の頂点を2つ以上の辺で結んだものであり，対応する地図で言うなら，2つの領域の境界の成分が2つ以上あり，その成分ごとに辺で結ぶという作業をすればできる．地図では実際このようなことが起きるが，彩色という意味からは不必要である．つまり，どれかの成分を選んで辺で結び，多重辺がないという条件を満たすように G を作り，G に対して頂点彩色が可能であることと元の地図が彩色可能であることは同値である．

ンの証明や，ロバートソン，サンダース，シーモア，トーマスによる最近（1997 年）の証明が成功したのは，（19 世紀に遡る）非常に古いアイデアと現代のコンピュータの非常に新しい計算力が結びついたお蔭である．もとの証明から 25 年が経っても基本的に状況は同じで，天書の証明は影すら見えない．

そこで少し謙虚になって，あらゆる平面グラフを 5 色で塗ることができることの簡潔な証明があるかどうかを問題にしよう．この 5 色定理の証明は，すでに世紀の変わり目[2]にヒーウッドによって与えられていた．彼の証明に対する（実際，4 色問題の証明のときも）基本的な道具はオイラーの公式である（第 10 章参照）．明らかに，グラフ G を彩色する際，G が連結であると仮定してもよい．もちろん，連結な部分ごとに色を塗っていけばよいからである．平面グラフは平面全体を（外側の領域を含む）領域の集合 R に分割する．オイラーの公式は，連結な平面グラフ $G=(V,E)$ に対して常に

$$|V|-|E|+|R| \;=\; 2$$

が成り立つというものである．



この平面グラフには 8 個の頂点，13 本の辺，7 つの領域がある．

手始めに，あらゆる平面グラフ G が 6 色で彩色可能であることの証明に，オイラーの公式がどのように使われるかを見てみよう．頂点の数 n に関する帰納法で行う．n の値が小さければ（特に $n \le 6$ であれば），これは明らかである．

86 ページの命題の (A) から，G には高々5 次の頂点 v のあることがわかっており，このことから G が 6 色で彩色可能であることがわかる．v と v につながっているすべての辺を取り除く．得られるグラフ $G' = G\backslash v$ は $n-1$ 個の頂点の上の平面グラフである．帰納法により，これは 6 色で彩色可能である．G の中で v と隣り合うのは高々5 つの頂点であり，G' の彩色の中でこれらの頂点には高々5 色しか使われていない．だから，G' の 6 色での彩色を，v と隣り合う頂点のどれにも使われていない色を v に使うことで，G の 6 色での彩色に拡張することができる．こうして，G は実際に 6 色で彩色可能になる．

ここで，ディニッツの問題についての章で述べた平面グラフのリスト彩色数を見てみよう．明らかに，上の 6 色での彩色の方法は色のリスト

[2] ［訳註］もちろん，19 世紀と 20 世紀の変わり目のことである．

に対しても有効で（またも色が足らなくなることはない），どんな平面グラフ G に対しても $\chi_\ell(G) \le 6$ となる．エルデシュ，ルービン，テイラーの3人は1979年に，あらゆる平面グラフのリスト彩色数は高々5であり，さらに $\chi_\ell(G) > 4$ を満たす平面グラフ G が存在すると予想した．その双方ともで彼らは正しかった．$\chi_\ell(G) = 5$ を満たす平面グラフの例を最初に作ったのはマルギット・ヴォイクトであるが（彼女の例には238個の頂点がある），ほとんど同時にカルステン・トーマッセンは5リスト彩色予想の真に驚くべき証明を与えた．彼の証明は，正しい帰納法の仮定を見つけようとするとき，何をすることができるのかという事情を教えてくれる例になっている．それはオイラーの公式をまったく使わないのである!

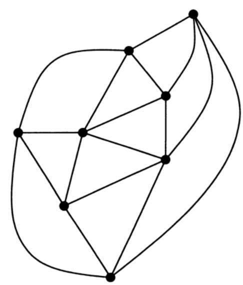
定理． **すべての平面グラフ G は5リスト彩色可能である．つまり，**

$$\chi_\ell(G) \le 5$$

という等式が成り立っている．

■ **証明．** まず，辺を増やすとき彩色数が減ることはないことに注意する．言い換えれば，H が G の部分グラフならば，確かに $\chi_\ell(H) \le \chi_\ell(G)$ が成り立つのである．それゆえ，G が連結なグラフで，平面への埋め込みの有界な面がすべて三角形であり，さらに有界でない面もある単純閉曲線（三角形でもよいし，より多くの頂点を持ってもよい）によって囲まれていると仮定してもよい．そのようなグラフを**概三角形分割された**グラフと呼ぼう．概三角形分割されたグラフに対する定理が正しければ，すべての平面グラフに対しても成り立つことになる．

証明のトリックは次のより強い主張を示すことである（そうすることで帰納法が使えるようになる）．



概三角形分割された平面グラフ．

$G = (V, E)$ を概三角形分割されたグラフで，B を外側の領域の境界となっているサイクルとする[3]．色の集合 $C(v)$，

[3] ［訳註］以下この証明の中では，B（とその部分集合）に対して，(1) 頂点の集合，(2) 辺の集合，(3) 頂点と辺（の実現）からなる点集合，という3つのあり方を，断らず使い分けている．どれかにこだわって解釈していると，数学的に誤りと感じる記述が出てくる．あえて個別に註を入れたり書き直したりしていないので注意すること．

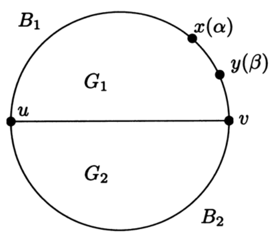
$v \in V$ に対して以下の仮定をする．

(1) B の隣り合う 2 頂点 x, y はすでに（異なる）色 α と β で塗られているとする．

(2) B の他のすべての頂点 v に対しては $|C(v)| \geq 3$ である．

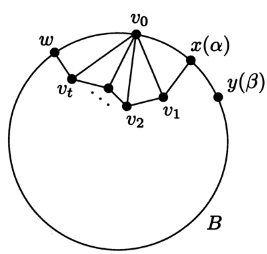
(3) 内部のすべての頂点 v に対しては $|C(v)| \geq 5$ である．

そのとき，リストの色をうまく選んで，x, y の彩色を G の彩色に拡張することができる．とくに，$\chi_\ell(G) \leq 5$ である．



$|V| = 3$ のときは明らかである．というのは，彩色されていない頂点 v はただ 1 つで，$|C(v)| \geq 3$ なのだから，使える色が残っているからである．さて，帰納法を始めよう．

場合 1. B に弦，つまり，2 頂点 $u, v \in B$ を結ぶ辺で B の中にないもの，が存在するとしよう．$B_1 \cup \{uv\}$ を境界とし，x, y, u, v を含む部分グラフ G_1 は概三角形分割されており，したがって帰納法の仮定から 5 リスト彩色可能である．この彩色で，頂点 u と v は色 γ と δ で塗られているとする．今度は，B_2 と uv を境界とする下側の部分 G_2 を考える．u, v があらかじめ彩色されていたとみなせば，帰納法の仮定は G_2 に対しても満たされていることがわかる．それゆえ，G_2 はまだ使える色を使って 5 リスト彩色可能であり，G に対しても同じことが成り立つ．



場合 2. B には弦がないとする．B 上，α 色が塗られている頂点 x のもう一方の側の頂点を v_0 とし，v_0 に隣り合う頂点を $x, v_1, \ldots, v_t, w$ とする．G は概三角形分割されているので，図に示したような状況になっている．

G から頂点 v_0 と v_0 から出ているすべての辺を取り除くと，概三角形分割されたグラフ $G' = G \backslash v_0$ が得られる．この G' の外側の境界は $B' = (B \backslash v_0) \cup \{v_1, \ldots, v_t\}$ である．仮定 (2) から $|C(v_0)| \geq 3$ であるので，$C(v_0)$ には α とは異なる 2 つの色 γ, δ が存在する．さて，色の集合 $C(v_i)$ はすべて $C(v_i) \backslash \{\gamma, \delta\}$ に替え，G' の他のすべての頂点に対しては元の色の集合そのままとする．すると，G' は明らかにすべての仮定を満たし，帰納法から 5 リスト彩色可能になる．v_0 には，γ と δ のうち，w に使われた色でない方を選べば，G' のリスト彩色は G 全体に

拡張することができる. □

5 リスト彩色定理は証明されたが，物語がお仕舞いというわけではない．もっと強い予想があるのだ．平面グラフ G のリスト彩色数は普通の彩色数より多くとも高々1 であるというものである．つまり，

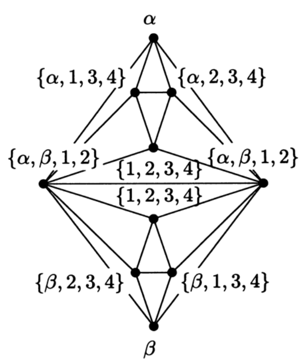
あらゆる平面グラフ G に対して $\chi_\ell(G) \le \chi(G)+1$ となるか？

4 色定理により $\chi(G) \le 4$ なのだから，起きるのは次の 3 つの場合である．

場合 I: $\chi(G)=2 \implies \chi_\ell(G) \le 3$,
場合 II: $\chi(G)=3 \implies \chi_\ell(G) \le 4$,
場合 III: $\chi(G)=4 \implies \chi_\ell(G) \le 5$.

トーマッセンの結果によって場合 III は成り立つ．場合 I はアロンとタルシにより巧妙な（そしてずっと高度な）議論によって証明された．さらに，$\chi(G)=2$ かつ $\chi_\ell(G)=3$ であるような平面グラフ G が存在する．たとえば，ディニッツの問題を扱った前章で考察したグラフ $K_{2,4}$ がそうである

では場合 II についてはどうなるだろう？ ここでは予想は間違っているのである．これを最初に示したのもマルギット・ヴォイクトで，シャイ・ガトナーが以前に構成していたグラフに対して示したのだが，そのグラフには 130 もの頂点がある．構成は以下のようにする．まず（余白の図の）「2 重の 8 面体」を考える．明らかにこれは 3 彩色可能である．$\alpha \in \{5,6,7,8\}$ かつ $\beta \in \{9,10,11,12\}$ とし，図に与えられたリストを考える．このリストでの彩色が不可能であることを確かめるのは読者に任そう．さて，このグラフのコピーを 16 個用意して，一番上のすべての頂点を同一視し，一番下のすべての頂点を同一視する．これで得られるグラフは，$16 \cdot 8+2=130$ 個の頂点を持ち，平面グラフであり，3 彩色可能である．上の頂点には $\{5,6,7,8\}$ を与え，下の頂点には $\{9,10,11,12\}$ を与える．さらに内部では，16 個の対 (α,β), $\alpha \in \{5,6,7,8\}$, $\beta \in \{9,10,11,12\}$ に対応するリストを与える．α と β をどのように選んでも，右の図のグラフを部分グラフとして含むので，この大きなグラフのリスト彩色は不可能である．



また別のガトナーの例を手直しして，ヴォイクトとワースはさらに小さい平面グラフを作った．頂点の数は 75 個，$\chi=3$ かつ $\chi_\ell=5$ を満た

し，合わせたリストが最小の5色だけを使うものである．現在の記録は63個の頂点を持つものである．

参考文献

[1] N. アロン，M. タルシ：「グラフの彩色と向き付け」(*Colorings and orientations of graphs*), Combinatorica **12** (1992), 125-134.

[2] P. エルデシュ，A. L. ルービン，H. テイラー：「グラフにおける選択可能性」(*Choosability in graphs*), Proc. West Coast Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium **26** (1979), 125-157.

[3] S. ガトナー：「平面グラフの選択可能性の複雑さ」(*The complexity of planar graph choosability*), Discrete Math. **159** (1996), 119-130.

[4] N. ロバートソン，D. P. サンダース， P. シーモア，R. トーマス:「4色定理」(*The four-colour theorem*), J. Combinatorial Theory, Ser. B **70** (1997), 2-44.

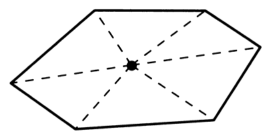
[5] C. トーマッセン:「あらゆる平面グラフは5選択可能である」(*Every planar graph is 5-choosable*), J. Combinatorial Theory, Ser. B **62** (1994), 180-181.

[6] M. ヴォイクト:「平面グラフのリスト彩色」(*List colorings of planar graphs*), Discrete Math. **120** (1993), 215-219.

[7] M. ヴォイクト，B. ワース:「3彩色可能だが4選択可能でない平面グラフについて」(*On 3-colorable non-4-choosable planar graphs*), J. Graph Theory **24** (1997), 233-235.

第28章　美術館の守り方

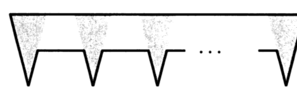
1973年にヴィクター・クリーによって提案された魅力的な問題がある．美術館の館長が，どんなときでも美術館のあらゆる地点が，ある警備員に監視されていることを確信していたいと思ったとする．警備員は一定の場所に配置されるが見廻すことはできるとする．何人の警備員が必要となるか？



凸な展示ホール．

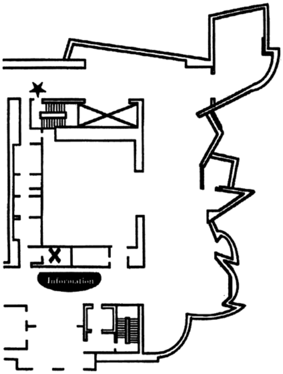
美術館の壁を n 個の辺からなる多角形として描く．もちろん，その多角形が凸なら1人の警備員で十分である．実際，警備員は美術館のどんな地点に配置してもよい． しかし一般には，美術館の壁はどんな閉多角形の形にもなり得るのである．

右の図に描かれたような $n=3m$ 枚の壁を持つ櫛の形をした美術館を考える．ここでは少なくとも $m=\frac{n}{3}$ 人の警備員が必要なことは容易にわかる．実際，n 枚の壁がある．1 の地点は，1 を含む影のついた三角形の中に配置された警備員によってのみ監視することが可能なこと，他の $2,3,\ldots,m$ という地点でも同様であることに注意する．これらすべての三角形は互いに交わらないので，少なくとも m 人の警備員が必要という結論になる．しかし，m 人の警備員で十分でもある．警備員を三角形の上の辺の所に配置することができるからである．三角形の先端部分の壁を1つか2つ切り落としてみれば，どんな n に対しても $\lfloor\frac{n}{3}\rfloor$ 人の警備員が必要な n 枚の壁を持つ美術館が存在するという結論が得られる．

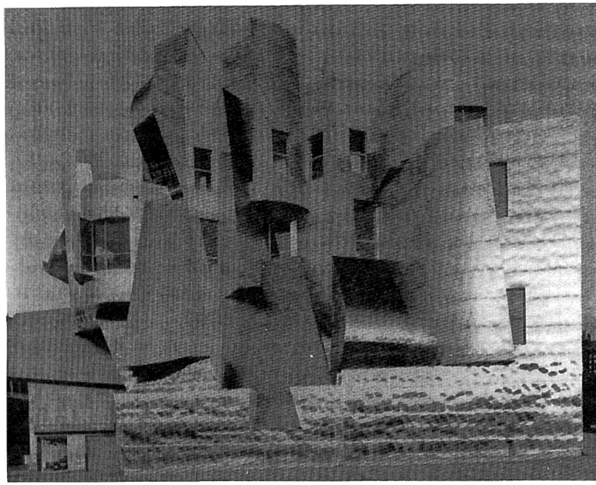


次の結果は，これが最悪の場合であることを示している．

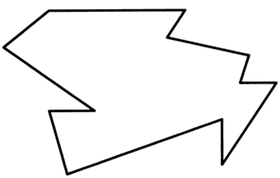
定理． n 枚の壁を持つどんな美術館でも $\lfloor\frac{n}{3}\rfloor$ 人の警備員がいれば十分である．



現実の美術館は . . . .

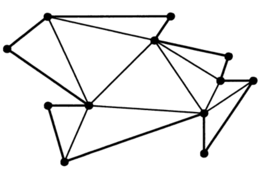


この「美術館定理」は最初ヴァシェック・ホヴァタルによって巧妙な議論で証明されたが，ここではスティーヴ・フィスクによる本当に美しい証明を述べよう．



壁が $n = 12$ 枚の美術館.

■ **証明.** まず最初に，壁の角の間の互いに交わらない対角線を $n-3$ 本引いて，内部が三角形分割されるようにしよう．たとえば，余白に描いた美術館では，9 本の対角線を引いて三角形分割することができる．どんな三角形分割を選んでも関係ないので，どれでもよい．さて，この新しい図形を，角を頂点とし，壁と対角線を辺とする平面グラフと考える．



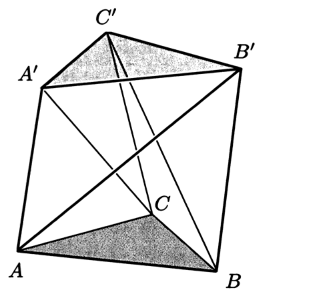
主張. このグラフは 3 彩色可能である.

$n = 3$ に対しては証明すべきことは何もない．そこで，$n > 3$ のときは対角線で結ばれている 2 頂点 u, v をとる．この対角線によって，グラフは 2 つの三角形分割された小さいグラフに分けられ，それらはともに辺 uv を持っている．帰納法により，各々の部分は 3 色で彩色することができ，各彩色で，u に対しては色 1 を，v に対しては色 2 を選んでよい．この彩色を貼り合わせれば，グラフ全体の 3 色での彩色が得られる．

残りは易しい．頂点の数は n だから，少なくとも 1 つの色の類には，

たとえば，色 1 で塗られた頂点の集合には，高々 $\lfloor \frac{n}{3} \rfloor$ 個の頂点が含まれることになり，この場所に警備員をおけばよい．あらゆる三角形は色 1 の頂点を持つので，あらゆる三角形は警備され，それゆえ美術館全体も警備される． □

明敏な読者なら，上の議論に微妙な点があることに気がついただろう．三角形分割は常に存在するのか？ おそらく誰もが最初は「もっちろん，あるさ！」と反応するだろう．そう，存在する．しかし，全く明らかなことというわけではないし，実際，3 次元への自然な一般化（4 面体への分割）は正しくないのである！ このことは余白に描いた**シェーンハルトの多面体**からわかるだろう．これは 1 つの三角プリズムから，その上面の三角形を回転させて得られたもので，四辺形の面はそれぞれ凸でない稜のところで 2 つの三角形に分かれている．この多面体を三角形分割してみよ！ 底面の三角形を含むどんな 4 面体も上面にある 3 つの頂点のどれか 1 つを含まなければならない．しかし，そのような 4 面体はシェーンハルトの多面体には含まれない．だから，頂点を付加しない限り三角形分割はあり得ないのである．

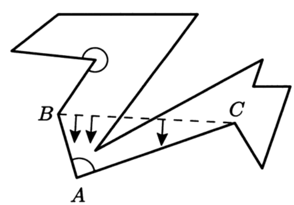


シェーンハルトの多面体． 稜 AB', BC', CA' での内側の面角は 180° より大きい．

凸でない平面の多角形の場合に三角形分割が存在することの証明を，頂点の数 n に関する帰納法で行う．$n = 3$ のとき多角形は三角形であり，証明すべきことはない．$n \geq 4$ としよう．帰納法を使うためにしなければならないことは，上でしたように，あとから貼り合わせることのできる 2 つの小部分に多角形 P を分けるような 1 つの対角線を作ることだけである．

頂点 A は，その頂点での内角が 180° より小さいとき，**凸**であると言う．P の内角の和は $(n-2)180°$ なので，凸な頂点 A がなければならない．実際，少なくとも 3 つは凸な頂点があるが，本質的にはこれは鳩の巣原理の応用である！ または，多角形の凸包を考えてもよく，そのすべての頂点はもとの多角形に対しても凸になっている[1]．

さて，A の隣の 2 つの頂点 B と C を見よう．線分 BC が P の中にすっぽり入れば，これが欲しかった対角線である．そうでなければ，三角形 ABC は別の頂点を含むことになる．BC を A に向かって滑らせていき，ABC の中にある最後の頂点 Z を通るようにする．すると，AZ

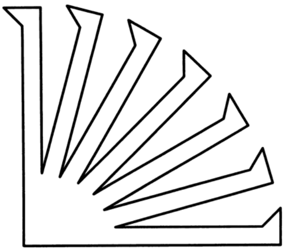


[1] ［訳註］凸包の頂点はもとの多角形の頂点でもあり，凸包をとる操作で内角が小さくなることはない．

は P の内部にあり，これが欲しかった対角線になる．

美術館定理を変形したものもたくさん考えられている．たとえば，壁だけを警備したい（結局のところ絵画か掛かっているのは壁なのだ）とか，警備員はすべて頂点に配置するとかである．とくに素敵な（そして未解決の）変形問題は次のものである．

各警備員は美術館の 1 つの壁をパトロールしてよいとする．
それで彼は自分の壁に沿って歩き，この壁沿いのある点から
見ることができるものは見えるとする．
そのとき，管理のために何人の「壁警備員」が必要か？



ゴットフリート・トゥサンは，ここに描いた美術館の例を作り，$\lfloor \frac{n}{4} \rfloor$ 人の警備員が必要だろうということを示した．

この多角形は 28 の辺（そして，一般には $4m$ 個の辺）を持っている．読者は m 人の壁警備員が必要であることを確かめてみて欲しい．n が小さいいくつかの値を除いて，この数が十分でもあると予想されているが，証明となると，天書の証明でないとしても，まだ何の見込みもない．

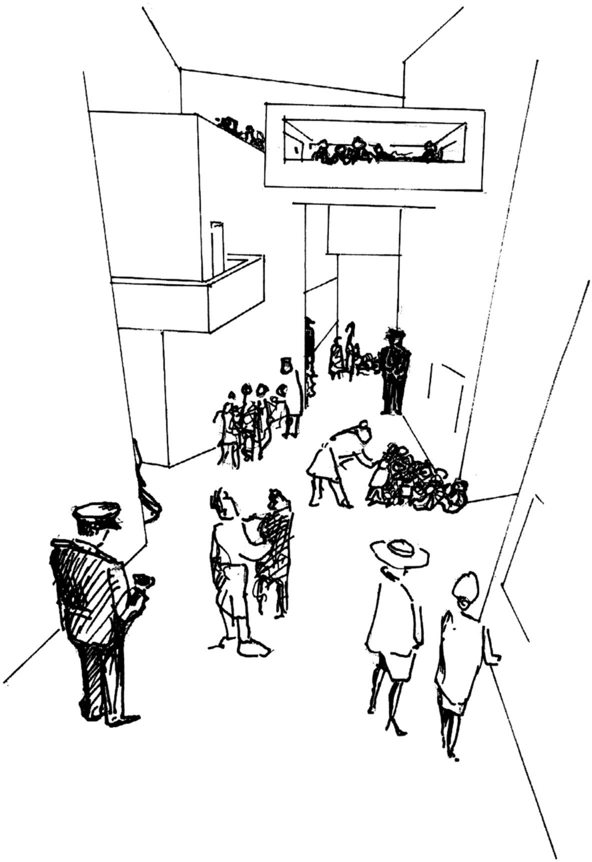
参考文献

[1] V. ホヴァタル：「平面幾何における組合せ論的定理」(*A combinatorial theorem in plane geometry*), J. Combinatorial Theory, Ser. B **18** (1975), 39-41.

[2] S. フィスク：「ホヴァタルの警備員定理の短い証明」(*A short proof of Chvátal's watchman theorem*), J. Combinatorial Theory, Ser. B **24** (1978), 374.

[3] J. オルーク：『美術館定理とアルゴリズム』(*Art Gallery Theorems and Algorithms*), Oxford University Press 1987.

[4] E. シェーンハルト：「3 角多面体の 4 面体への分解について」(*Über die Zerlegung von Dreieckspolyedern in Tetraeder*), Math. Annalen **98** (1928), 309-312.



「美術館の警備」
(3 次元の美術館問題)

第29章　トゥラーンのグラフ定理

グラフ理論の基本結果の1つは1941年のトゥラーンの定理で，これが極値的グラフ理論の始まりとなった．トゥラーンの定理は何度も再発見され，さまざまな異なる証明が得られている．そのうちの5つを述べ，読者に，どれが天書にあるべき証明かを決めていただくことにする．

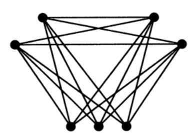
まず記号を固定する．頂点の集合 $V = \{v_1, \ldots, v_n\}$ と辺の集合 E の単純グラフ G を考える．v_i と v_j が隣り合っているとき，$v_iv_j \in E$ と書く．G における p **クリーク**とは，G の部分グラフで p 個の頂点上の完全グラフになっているもののことで，K_p と書く．ポール・トゥラーンは次の問題を提案した．



ポール・トゥラーン

G は p クリークを含まない単純グラフであるとする． G が持ち得る辺の最大数はいくつか？

V が $p-1$ 個の互いに交わらない部分集合 $V = V_1 \cup \cdots \cup V_{p-1}$, $|V_i| = n_i, n = n_1 + \cdots + n_{p-1}$ に分かれ，2つの頂点が結ばれることが，異なる集合 V_i, V_j に属することと同値だという例はたやすく得ることができる．そのようなグラフを $K_{n_1,\ldots,n_{p-1}}$ と書くと，辺の数は $\sum_{i<j} n_in_j$ である．n が与えられたとき，できるだけ一様に，つまりすべての i, j に対して $|n_i - n_j| \leq 1$ を満たすように数 n_i に分けたなら，そのようなグラフの中から辺の数が最大なものが得られる．実際，$n_1 \geq n_2 + 2$ と仮定しよう．V_1 から V_2 に頂点を1つ動かしたら $K_{n_1-1,n_2+1,\ldots,n_{p-1}}$ が得られ，辺の数は $K_{n_1,n_2,\ldots,n_{p-1}}$ より，$(n_1-1)(n_2+1) - n_1n_2 = n_1 - n_2 - 1 \geq 1$ 本多い．$|n_i - n_j| \leq 1$ を満たすグラフ $K_{n_1,\ldots,n_{p-1}}$ をトゥラーン・



グラフ $K_{2,2,3}$.

グラフと言う．とくに，$p-1$ が n の約数なら，すべての i に対して $n_i = \frac{n}{p-1}$ とおいてよく，そのときの辺の数は

$$\binom{p-1}{2}\left(\frac{n}{p-1}\right)^2 = \left(1-\frac{1}{p-1}\right)\frac{n^2}{2}$$

である．トゥラーンの定理は，この数が，n 個の頂点の上の p クリークを持たないどんなグラフの辺の数に対しても上界になっているという主張である．

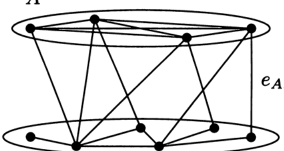
定理． **n 個の頂点の上のグラフ $G=(V,E)$ が p クリーク ($p \geq 2$) を持たなければ，**

$$|E| \leq \left(1-\frac{1}{p-1}\right)\frac{n^2}{2} \tag{1}$$

を満たす．

$p=2$ のときは自明である．最初の興味ある場合である $p=3$ のとき，定理が言っているのは，n 個の頂点の上の三角形を含まないグラフは高々 $\frac{n^2}{4}$ 個の辺しか含まないということである．この特殊な場合の証明はトゥラーンの結果より前に知られていた．不等式を使った 2 つのエレガントな証明が第 16 章にある．

一般の場合に移ろう．最初の 2 つの証明は帰納法を使い，それぞれトゥラーンとエルデシュによるものである．



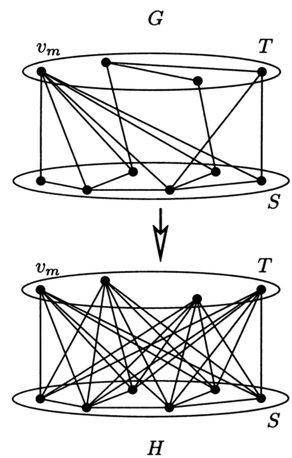
■ **第 1 の証明．** n に関する帰納法を使う．$n \leq p-1$ に対して (1) が正しいことは容易に計算される．そこで $n \geq p$ と仮定し，G が $V=\{v_1,\ldots,v_n\}$ の p クリークを持たないグラフで，辺の数が最大のものとする．G は必ず $(p-1)$ クリークを持つ．そうでないなら，辺を追加できるからである．A を $(p-1)$ クリークとし，$B=V\backslash A$ とおく．

A は $\binom{p-1}{2}$ 個の辺を含む．そこで，B の中の辺の数 e_B と，A と B との間の辺の数 $e_{A,B}$ を評価しよう．帰納法によって $e_B \leq \frac{1}{2}(1-\frac{1}{p-1})(n-p+1)^2$ が得られる．G には p クリークはないから，あらゆる $v_j \in B$ は，A の中の高々 $p-2$ 個の頂点としかつながらないので，$e_{A,B} \leq (p-2)(n-p+1)$ が得られる．全部合せると，

$$|E| \leq \binom{p-1}{2} + \frac{1}{2}\left(1-\frac{1}{p-1}\right)(n-p+1)^2 + (p-2)(n-p+1)$$

となり，これはちょうど $(1-\frac{1}{p-1})\frac{n^2}{2}$ である． □

■ **第 2 の証明.** この証明はトゥラーン・グラフの構造を使う．$v_m \in V$ を最大次数 $d_m = \max_{1\le j\le n} d_j$ の頂点とする．v_m に隣り合う点の集合を S とすると $|S| = d_m$ であり，$T = V\backslash S$ とおく．G が p クリークを含まず，v_m は S のすべての頂点と隣り合うので，S は $(p-1)$ クリークを含まないことを注意する．



そこで次のような V 上のグラフ H を作る（図を見よ）．H は S 上では G に対応し，S と T の間のすべての辺を含み，T の中では辺を持たないものである．言い換えれば，H において T は独立な集合で，H はまた p クリークを含まないことが結論される．d'_j を H における v_j の次数とする．もし $v_j \in S$ ならば，H の構成から $d'_j \ge d_j$ となり，$v_j \in T$ に対しては，v_m の選び方から，$d'_j = |S| = d_m \ge d_j$ となる．$|E(H)| \ge |E|$ がわかり，辺の数が最大のグラフ全体の中には H の形をしたものがあることがわかる．帰納法により，S によって誘導されたグラフには，S 上の適当なグラフ $K_{n_1,\dots,n_{p-2}}$ と同じ数の辺しかないことになる．だから，$n_{p-1} = |T|$ として，$|E| \le |E(H)| \le E(K_{n_1,\dots,n_{p-1}})$ となり，これから (1) が得られる． □

次の 2 つの証明は全く異なった性格のもので，確率論の最大化の議論とアイデアを使うものである．それらはそれぞれ，モツキンとシュトラウス，そしてアロンとスペンサーによるものである．

■ **第 3 の証明.** 頂点の上の**確率分布** $\boldsymbol{w} = (w_1,\dots,w_n)$ を考える．つまり，頂点に $\sum_{i=1}^n w_i = 1$ を満たす値 $w_i \ge 0$ を与える．関数

$$f(\boldsymbol{w}) \;=\; \sum_{v_iv_j\in E} w_iw_j$$

を最大にすることを目的とする．$\boldsymbol{w}$ を任意の分布とし，v_i と v_j を重み w_i, w_j が正の，隣り合わない頂点の対とする．s_i を v_i に隣り合うすべての頂点の重みの和とし，v_j に対して同様に s_j を定義する．$s_i \ge s_j$ と仮定してよい．そこで，v_j から v_i に重みを移す．つまり，v_i の新しい重みを $w_i + w_j$ とし，v_j の重みを 0 に落とす．この新しい分布 $\boldsymbol{w}'$ に対しては

$$f(\boldsymbol{w}') \;=\; f(\boldsymbol{w}) + w_js_i - w_js_j \;\ge\; f(\boldsymbol{w})$$



「重みを動かして」

となる．このステップを繰り返すと（各ステップで重みが正の頂点の数は少なくなる），0 でない重みが，あるクリーク，たとえばある k クリークに集中しているような最適な分布が存在するという結論になる．今度は，たとえば $w_1 > w_2 > 0$ であれば，$0 < \varepsilon < w_1 - w_2$ を満たす ε を選んで，w_1 を $w_1 - \varepsilon$ に，w_2 を $w_2 + \varepsilon$ に変える．新しい分布 $\boldsymbol{w}'$ は $f(\boldsymbol{w}') = f(\boldsymbol{w}) + \varepsilon(w_1 - w_2) - \varepsilon^2 > f(\boldsymbol{w})$ を満たし，f の最大値が，ある k クリークの上で $w_i = \frac{1}{k}$ であり，他では $w_i = 0$ であるものに対してとられることがわかる．1 つの k クリークには $\frac{k(k-1)}{2}$ 本の辺があるので，

$$f \;=\; \frac{k(k-1)}{2}\frac{1}{k^2} \;=\; \frac{1}{2}\Big(1 - \frac{1}{k}\Big)$$

となる．この表示は k に関して増加しているので，一番よいのは $k = p-1$ とおくことである（G は p クリークを持たないからである）．だから，どんな分布 $\boldsymbol{w}$ に対しても

$$f(\boldsymbol{w}) \;\leq\; \frac{1}{2}\Big(1 - \frac{1}{p-1}\Big)$$

という結論がでる．とくに，この不等式は，すべての i に対し $w_i = \frac{1}{n}$ によって与えられる**一様分布**に対しても成り立つ．つまり，

$$\frac{|E|}{n^2} \;=\; f\Big(w_i = \frac{1}{n}\Big) \;\leq\; \frac{1}{2}\Big(1 - \frac{1}{p-1}\Big)$$

が成り立つが，これはまさに (1) そのものである．　□

■ **第 4 の証明.** 今度は確率論の概念をいくつか使う．G を，頂点集合 $V = \{v_1, \ldots, v_n\}$ 上の任意のグラフとする．v_i の次数を d_i と表わし，最大のクリークの頂点の数を $\omega(G)$ と書き，G の**クリーク数**と呼ぶ．

主張. $\omega(G) \;\geq\; \displaystyle\sum_{i=1}^{n} \frac{1}{n - d_i}$ **が成り立つ.**

V のランダムな置換 $\pi_1\pi_2\cdots\pi_n$ を等確率 $\frac{1}{n!}$ で選び，次の集合 C_π を構成する．π_i が C_π に属するのは，π_i の前にいるすべての π_j $(j < i)$ と π_i が隣り合うときとする．定義により，C_π は G のクリークである．$X = |C_\pi|$ を対応する確率変数とする．X_i を頂点 v_i の特性確率変数，つまり，$v_i \in C_\pi$ か $v_i \notin C_\pi$ かに従って $X_i = 1$ か $X_i = 0$ とするとき，

$X = \sum_{i=1}^{n} X_i$ となっている．v_i が置換 $\pi_1\pi_2\cdots\pi_n$ に関して C_π に属するのは，v_i が v_i に隣り合わない $n-1-d_i$ 個のすべての頂点の前にいるとき，言い換えれば，v_i とそれに隣り合わない $n-1-d_i$ 個の頂点の中で一番前にいるとき，かつそのときに限ることに注意する．このことが起こる確率は $\frac{1}{n-d_i}$ であり，それゆえ $EX_i = \frac{1}{n-d_i}$ となる．

こうして，期待値の線形性（112 ページ参照）から

$$E(|C_\pi|) \;=\; EX \;=\; \sum_{i=1}^{n} EX_i \;=\; \sum_{i=1}^{n} \frac{1}{n-d_i}$$

が得られる．結果として，少なくともこのサイズのクリークが存在しなければならず，これは上の主張になっている．この主張からトゥラーンの定理を導くために，第 16 章のコーシー–シュヴァルツの不等式

$$\Big(\sum_{i=1}^{n} a_i b_i\Big)^2 \;\le\; \Big(\sum_{i=1}^{n} a_i^2\Big)\Big(\sum_{n=1}^{n} b_i^2\Big)$$

を使う．$a_i = \sqrt{n-d_i}$, $b_i = \frac{1}{\sqrt{n-d_i}}$ とおけば $a_i b_i = 1$ であり，だから

$$n^2 \;\le\; \left(\sum_{i=1}^{n}(n-d_i)\right)\left(\sum_{i=1}^{n}\frac{1}{n-d_i}\right) \;\le\; \omega(G)\sum_{i=1}^{n}(n-d_i) \qquad (2)$$

となる．ここでトゥラーンの定理の仮定 $\omega(G) \le p-1$ を使う．また，2 重数え上げの章の公式 $\sum_{i=1}^{n} d_i = 2|E|$ を使うと，不等式 (2) は

$$n^2 \;\le\; (p-1)(n^2 - 2|E|)$$

となるが，これはトゥラーンの不等式と同値である． □

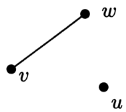
さて，最後の証明に取り掛かろう．おそらく一番美しい証明かもしれない．誰から出たものか，はっきりしない．私たちはシュテファン・ブラントから教えてもらったが，彼はオーベルヴォルファッハ[1]で聞いたという.「民間伝承」のグラフ理論と言うべきかも知れない．トゥラーン・グラフが実際上，辺の数が最大の唯一の例であることを一挙に示してく

---

[1] ［訳註］ドイツ南部のいわゆる黒い森の中にある小さい村（オーベルヴォルファッハ）に数学の研究所が建っている．毎週テーマが変わり，テーマごとに世界中から招待された研究者によってセミナーが開かれている．常駐するスタッフはごく少ないが，恩恵を受けた数学者は多い．夕食のあとは飲み物も出て，ホールや庭で語り合っている．

れる証明である．証明の 1 と 2 からでもこの強い結果が示されることは注意しておいた方がよいだろう．

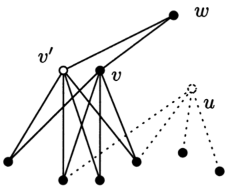
■ **第 5 の証明.** G を n 個の頂点上の p クリークを持たないグラフで，辺の数が最大のものとする．



> **主張. G は，$vw \in E$ だが，$uv \notin E$, $uw \notin E$ であるような 3 つの頂点 u, v, w を含まない.**

そうでなかったと仮定し，次の 2 つの場合を考える．

場合 1. $d(u) < d(v)$　または　$d(u) < d(w)$.



$d(u) < d(v)$ と仮定してよい．このとき，v を複製し，つまり新しい頂点 v' を作ってつながり方は v と同じにし（vv' は辺にしない），u を消して，残りは変えないでおく．

新しいグラフ G' も p クリークは持たず，辺の数は

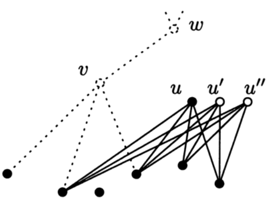
$$|E(G')| \;=\; |E(G)| + d(v) - d(u) \;>\; |E(G)|$$

となる．これは矛盾である．

場合 2. $d(u) \geq d(v)$　かつ　$d(u) \geq d(w)$.

u を 2 つ複製し，v と w を消す．今度も新しいグラフ G' は p クリークは持たず，

$$|E(G')| \;=\; |E(G)| + 2d(u) - (d(v) + d(w) - 1) \;>\; |E(G)|$$



と計算される（-1 は辺 vw の分である）．だからまた矛盾が出る（余白の図の説明のように）．

少し考えればわかることだが，上で示した主張は，

$$u \sim v \iff uv \notin E(G)$$

が同値関係を定めることと同値である．こうして，G は完全多部グラフ $G = K_{n_1,\dots,n_{p-1}}$ となり，証明は終わる．□

参考文献

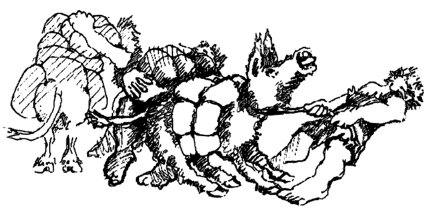
[1] M. アイグナー：「トゥラーンのグラフ定理」(*Turán's graph theorem*), Amer. Math. Monthly **102** (1995), 808-816.

[2] N. アロン, J. スペンサー：『確率論的方法』(*The Probabilistic Method*), Wiley Interscience 1992.

[3] P. エルデシュ：「トゥラーンのグラフ定理について」(*On the graph theorem of Turán*)（ハンガリー語）, Math. Fiz. Lapok **21** (1970), 249-251.

[4] T. S. モツキン, E. G. シュトラウス：「グラフにおける最大値とトゥラーンの定理の新証明」(*Maxima for graphs and a new proof of a theorem of Turán*), Canad. J. Math. **17** (1965), 533-540.

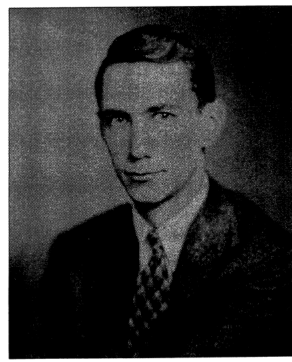
[5] P. トゥラーン：「グラフ理論における極値問題について」(*On an extremal problem in graph theory*), Math. Fiz. Lapok **48** (1941), 436-452.



「動かす重みはもっと多く」

第30章　誤りのない通信

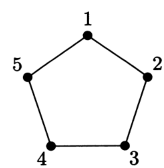
情報理論の開祖であるクロード・シャノンは，1956 年に次の非常に興味深い問題を提案した．



クロード・シャノン

メッセージを，(いくつかのシンボルが歪(ひず)むかも知れない) チャンネルを通して受信者に伝送したいとしよう．受信者がもとのメッセージを間違いなく再現できるような最大の伝送速度はいくつか？

シャノンの使う「チャンネル（情報路)」や「伝送速度」の意味を見てみよう．シンボルの集合 V が与えられていて，メッセージは V のシンボルの列であるとする．チャンネルのモデルをグラフ $G = (V, E)$ として，V はシンボルの集合で，E はシンボルの信頼できない対の間の辺の集合とする．つまり，シンボルは伝送の間に混乱するかも知れないとする．たとえば，日常会話で電話で通信していると，シンボル B と P をつなぐことになる．というのは，受信者がこの 2 つを区別できないかも知れないからである．この G を**混乱グラフ**と呼ぼう．



この議論では 5 サイクル C_5 が目立った働きをする．この例では，1 と 2 は取り違えるかも知れないが，1 と 3 では混乱は起こらない，などとなる．理想的には，5 つのシンボルすべてを通信に使いたいが，誤りのない通信をしたいので，単独のシンボル達を送るだけなら，混乱を起こすかも知れない対のそれぞれからは 1 文字しか使うことができない．つまり，この 5 サイクルに対しては，異なる 2 文字（辺で結ばれていない任意の 2 つ）しか使うことができない．情報理論の言葉では，このことを，この 5 サイクルに対しては，(最大の $\log_2 5 \approx 2.32$ ではなく) $\log_2 2 = 1$ の情報速度を達成すると言う．明らかにこのモデルでは，任意のグラフ

$G=(V,E)$ に対して，なし得る最善のことは 1 つの最大の独立集合のシンボルを通信することである．つまり，1 つのシンボルを送るときの情報速度は $\log_2\alpha(G)$ である．ただし，$\alpha(G)$ は G の**独立数**である．

1 つのシンボルの代わりにその列を使うことによって情報速度を大きくすることができるかどうかを見てみよう．長さ 2 の文字列を送信したいとしよう．列 u_1u_2 と v_1v_2 が混乱する可能性があるのは次の 3 つの場合のどれかが成り立つときだけである．

- $u_1=v_1$ であり，u_2 が v_2 と混乱し得る．
- $u_2=v_2$ であり，u_1 が v_1 と混乱し得る．
- $u_1\neq v_1$ が混乱し，$u_2\neq v_2$ が混乱し得る．

グラフ理論の言葉では，このことは 2 つのグラフ $G_1=(V_1,E_1)$ と $G_2=(V_2,E_2)$ の**積** $G_1\times G_2$ を考えることになる．$G_1\times G_2$ の頂点集合は $V_1\times V_2=\{(u_1,u_2):u_1\in V_1,u_2\in V_2\}$ で，$(u_1,u_2)\neq(v_1,v_2)$ が辺で結ばれるのは，$i=1,2$ に対し $u_i=v_i$ または $u_iv_i\in E$ が成り立つときである．こうして，長さ 2 の文字列に対する混乱グラフはグラフ G と自分自身との積 $G^2=G\times G$ である．このとき，長さ 2 の文字列の（**シンボルあたりの**）情報速度は

$$\frac{\log_2\alpha(G^2)}{2} \;=\; \log_2\sqrt{\alpha(G^2)}$$

で与えられる．ここで，もちろん，任の長さ n の文字列を使ってもよいだろう．n 次混乱グラフ $G^n=G\times G\times\cdots\times G$ の頂点集合は $V^n=\{(u_1,\ldots,u_n):u_i\in V\}$ であり，$(u_1,\ldots,u_n)\neq(v_1,\ldots v_n)$ はすべての i に対して $u_i=v_i$ または $u_iv_i\in E$ が満たされるとき辺で結ばれる．長さ n の文字列によって定まるシンボルあたりの情報速度は

$$\frac{\log_2\alpha(G^n)}{n} \;=\; \log_2\sqrt[n]{\alpha(G^n)}$$

である．

$\alpha(G^n)$ についてどんなことが言えるだろうか？ 少し様子を見てみよう．$U\subseteq V$ を G における最大の独立集合として，$|U|=\alpha$ とおく．すべての i に対して $u_i\in U$ を満たす $(u_1,\ldots,u_n)$ の形の α^n 個の G^n の頂点は，明らかに G^n の中の独立集合になっている．それゆえ，

$$\alpha(G^n) \geq \alpha(G)^n$$

であり，したがって

$$\sqrt[n]{\alpha(G^n)} \geq \alpha(G)$$

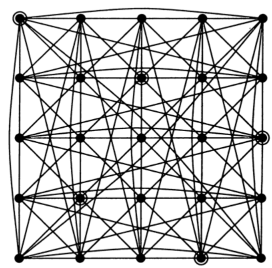
となり，1 つのシンボルの代わりにより長い列を使っても情報速度が減ることはないことになる．ついでに言えば，このことは符号理論の基本的なアイデアである．つまり，シンボルをより長い文字列に符号化することによって，誤りのない通信をより効果的に行うことができるのである．

対数を無視すれば，シャノンの基本的な定義が得られる．グラフ G の**誤りゼロ容量**は

$$\Theta(G) = \sup_{n \geq 1} \sqrt[n]{\alpha(G^n)}$$

によって与えられ，シャノンの問題は $\Theta(G)$ を，とくに $\Theta(C_5)$ を計算することであった．

C_5 を見てみよう．これまでのところ $\alpha(C_5) = 2 \leq \Theta(C_5)$ がわかっている．前に描いた 5 サイクルか，余白に描いた積 $C_5 \times C_5$ を見てみると，集合 $\{(1,1),(2,3),(3,5),(4,2),(5,4)\}$ が ${C_5}^2$ の中で独立であることがわかる．だから $\alpha({C_5}^2) \geq 5$ である．独立な集合は，連続した 2 つの行からは 2 つの頂点しか含み得ないので，$\alpha({C_5}^2) = 5$ がわかる．それゆえ，長さ 2 の文字列を使うことにより，容量に対する下界を $\Theta(C_5) \geq \sqrt{5}$ にまで大きくできたのである．



グラフ $C_5 \times C_5$.

これまでは容量に対する上界は得られていない．上界を得るために，もう一度シャノンのもとのアイデアに従うことにする．まず，独立集合の双対な定義は必要である．部分集合 $C \subseteq V$ が**クリーク**であるとは，C の任意の頂点が辺で結ばれるときに言うのであった．つまり，頂点はサイズ 1 の自明なクリークをなし，辺はサイズ 2 のクリークであり，三角形はサイズ 3 のクリークであり，などとなっている．$\mathcal{C}$ を G のクリークの集合とする．頂点集合上に任意の確率分布 $\boldsymbol{x} = (x_v : v \in V)$ を，つまり，$x_v \geq 0$ と $\sum_{v \in V} x_v = 1$ を満たすものを考える．それぞれの分布 $\boldsymbol{x}$ に,「クリークの最大値」

$$\lambda(\boldsymbol{x}) = \max_{C \in \mathcal{C}} \sum_{v \in C} x_v$$

を対応させ，最後に

$$\lambda(G) \;=\; \min_{\boldsymbol{x}} \lambda(\boldsymbol{x}) \;=\; \min_{\boldsymbol{x}} \max_{C\in\mathcal{C}} \sum_{v\in C} x_v$$

とおく．厳密には min に代わりに inf を使うべきだが，$\lambda(\boldsymbol{x})$ はすべての分布のなすコンパクト集合上で連続なので，最小値が存在する．

さて，独立集合 $U \subseteq V$ でサイズが最大の $\alpha(G) = \alpha$ であるものを考えよう．U に対し，分布 $\boldsymbol{x}_U = (x_v : v \in V)$ を，$v \in U$ ならば $x_v = \frac{1}{\alpha}$ とおき，それ以外は $x_v = 0$ とおいて定義する．どんなクリークも U の頂点は高々1 つしか含まないので，$\lambda(\boldsymbol{x}_U) = \frac{1}{\alpha}$ と推論され，こうして $\lambda(G)$ の定義から

$$\lambda(G) \le \frac{1}{\alpha(G)} \qquad \text{つまり} \qquad \alpha(G) \le \lambda(G)^{-1}$$

となる．シャノンが考えたことは，$\lambda(G)^{-1}$ が実際，すべての $\sqrt[n]{\alpha(G^n)}$ に対する上界であり，それゆえ $\Theta(G)$ に対しても上界であるということである．このことを証明するには，グラフ G, H に対して，

$$\lambda(G \times H) \;=\; \lambda(G)\lambda(H) \tag{1}$$

が成り立つことを示せばよい．なぜなら，このことから $\lambda(G^n) = \lambda(G)^n$ が導かれ，それゆえ，

$$\alpha(G^n) \le \lambda(G^n)^{-1} = \lambda(G)^{-n} \quad \text{つまり} \quad \sqrt[n]{\alpha(G^n)} \le \lambda(G)^{-1}$$

が得られるからである．(1) を証明するために，線形プログラミングの双対定理（[1] を参照）を使って，

$$\lambda(G) \;=\; \min_{\boldsymbol{x}} \max_{C\in\mathcal{C}} \sum_{v\in C} x_v \;=\; \max_{\boldsymbol{y}} \min_{v\in V} \sum_{C\ni v} y_C \tag{2}$$

を得る．ここで右辺は $\mathcal{C}$ 上のすべての確率分布 $\boldsymbol{y} = (y_C : C \in \mathcal{C})$ を走っている．

$G \times H$ を考え，$\boldsymbol{x}$ と $\boldsymbol{x}'$ をそれぞれ最小値 $\lambda(\boldsymbol{x}) = \lambda(G)$, $\lambda(\boldsymbol{x}') = \lambda(H)$ を与える分布とする．$G \times H$ の頂点集合では，頂点 (u, v) に $z_{(u,v)} = x_u x'_v$ という値を与える．$\sum_{(u,v)} z_{(u,v)} = \sum_u x_u \sum_v x'_v = 1$ であるから，分布が得られている．次に，$G \times H$ の最大のクリークが $C \times D = \{(u, v) : u \in C, v \in D\}$ で，C と D がそれぞれ G と H で

のクリークであるという形をしていることになる．それゆえ，$\lambda(G\times H)$ の定義により，

$$\begin{aligned}\lambda(G\times H)\ \le\ \lambda(z) &= \max_{C\times D}\sum_{(u,v)\in C\times D} z_{(u,v)}\\ &= \max_{C\times D}\sum_{u\in C} x_u \sum_{v\in D} x'_v\ =\ \lambda(G)\lambda(H)\end{aligned}$$

が得られる．同じようにして，$\lambda(G)$ に対する (2) の双対な表示を使うことによって，逆の不等式 $\lambda(G\times H)\ge\lambda(G)\lambda(H)$ を容易に示すことができる．まとめると，任意のグラフ G に対して，

$$\Theta(G)\ \le\ \lambda(G)^{-1}$$

を主張することができる．

発見したことを 5 サイクル，そしてもっと一般に m サイクル C_m に適用しよう．頂点の上の一様分布 $(\frac{1}{m},\ldots,\frac{1}{m})$ を使うことによって $\lambda(C_m)\le\frac{2}{m}$ が得られるのは，どんなクリークも高々2 頂点しか含まないからである．同じようにして，辺には $\frac{1}{m}$ を与え，頂点には 0 とすると，(2) の双対な表示により，$\lambda(C_m)\ge\frac{2}{m}$ であることがわかる．$\lambda(C_m)=\frac{2}{m}$ が結論されるので，すべての m に対して，

$$\Theta(C_m)\ \le\ \frac{m}{2}$$

となる．さて，m が偶数なら，明らかに $\alpha(C_m)=\frac{m}{2}$ であり，$\Theta(C_m)=\frac{m}{2}$ ともなる．しかし，m が奇数なら，$\alpha(C_m)=\frac{m-1}{2}$ となる．$m=3$ のときは C_3 はクリークであり，だからあらゆる積 C_3^n もクリークで，$\alpha(C_3)=\Theta(C_3)=1$ が得られる．だから，興味のある最初の場合は 5 サイクルで，これまでのところでわかっているのは

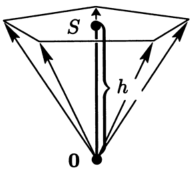
$$\sqrt{5}\ \le\ \Theta(C_5)\ \le\ \frac{5}{2} \tag{3}$$

である．

シャノンはその線形プログラミング的アプローチ（と他のいくつかのアイデア）を使って，多くのグラフの容量を，とくに頂点数が 5 以下のすべてのグラフの容量を計算することができた．ただし，これには 1 つだけ例外があって，それが C_5 であり，そのときに (3) の限界を超えることは彼にはできなかった．物事はここに 20 年以上も留まったまま

だったが，ついにラースロー・ロヴァースが驚くほど単純な議論で実際に $\Theta(C_5) = \sqrt{5}$ であることを示した．非常に難しく見えた組合せの問題に予期せぬ美しい解があったのである．

ロヴァースの主たる新しいアイデアは，グラフの頂点を長さ 1 の実ベクトルで表わし，その際，G の隣接しない 2 頂点に属する 2 つのベクトルが直交するようにすることである．そのようなベクトルの集合を G の**正規直交表現**と呼ぼう．明らかにそのような表現は常に存在する．次元 $m = |V|$ の単位ベクトル $(1,0,\ldots,0)^T$, $(0,1,0,\ldots,0)^T$, $\ldots$, $(0,0,\ldots,1)^T$ をとればよいからである．



ロヴァースの傘．

グラフ C_5 のときは，長さ 1 の 5 本の骨 $\boldsymbol{v}_1,\ldots,\boldsymbol{v}_5$ を持った「傘」を考えることによって，$\mathbb{R}^3$ における正規直交表現が得られる．そこで，傘を（先端を原点において），1 つおきの骨の間の角が 90° になるまで，開いていけばよい．

それからロヴァースは，傘の高さ h，つまり $\mathbf{0}$ と S との間の距離を使った上からの評価

$$\Theta(C_5) \leq \frac{1}{h^2} \tag{4}$$

を示すことに進んでいった．

簡単な計算によって $h^2 = \frac{1}{\sqrt{5}}$ であることがわかる（次ページの箱を参照）．これから，$\Theta(C_5) \leq \sqrt{5}$ であることが，さらに $\Theta(C_5) = \sqrt{5}$ であることがわかる．

ロヴァースが不等式 (4) をどのようにして証明していったかを説明しよう（彼の結果は実はずっと一般なものである）．$\mathbb{R}^s$ の 2 つのベクトル $\boldsymbol{x} = (x_1,\ldots,x_s)$, $\boldsymbol{y} = (y_1,\ldots,y_s)$ の通常の内積

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = x_1y_1 + \cdots + x_sy_s$$

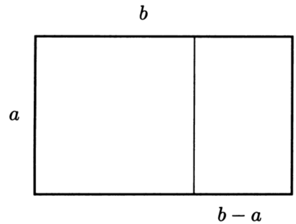
を考える．そのとき，$|\boldsymbol{x}|^2 = \langle \boldsymbol{x}, \boldsymbol{x} \rangle = x_1^2 + \cdots + x_s^2$ は $\boldsymbol{x}$ の長さ $|\boldsymbol{x}|$ の 2 乗であり，$\boldsymbol{x}$ と $\boldsymbol{y}$ の間の角は

$$\cos\gamma = \frac{\langle \boldsymbol{x}, \boldsymbol{y} \rangle}{|\boldsymbol{x}||\boldsymbol{y}|}$$

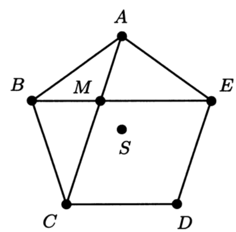
によって与えられる．こうして，$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ であることと，$\boldsymbol{x}$ と $\boldsymbol{y}$ が直交することが同値になる．

正 5 角形と黄金比

（図のように）長さ a の正方形を切り取って残る長方形がもとの長方形と同じ形をしている長方形を，美的に好ましいと考える伝統がある．そのような長方形の辺の長さ a, b は $\frac{b}{a} = \frac{a}{b-a}$ を満たさなければならない．その比を $\tau = \frac{b}{a}$ とおくと，$\tau = \frac{1}{\tau-1}$ が，つまり $\tau^2 - \tau - 1 = 0$ が得られる．この 2 次方程式を解けば，**黄金比** $\tau = \frac{1+\sqrt{5}}{2} \approx 1.6180$ が得られる．



今度は辺の長さが a の正 5 角形を考え，d を対角線の長さとする．$\frac{d}{a} = \tau$ であり，2 つの対角線の交点が対角線を黄金比に分割することは，すでにユークリッド（『原論』XIII, 8）にも知られていた．ユークリッドの天書の証明を述べる．5 角形の内角の和は 3π だから，各頂点での内角は $\frac{3\pi}{5}$ になる．ABE は二等辺三角形だから，$\sphericalangle ABE = \frac{\pi}{5}$ である．するとこれから $\sphericalangle AMB = \frac{3\pi}{5}$ がわかり，三角形 ABC と AMB が相似であることがわかる．四辺形 $CMED$ は，対辺が平行だから（角をみよ），菱形であり，だから $|MC| = a$ となり，$|AM| = d - a$ となる．ABC と AMB は相似だから，



$$\frac{d}{a} = \frac{|AC|}{|AB|} = \frac{|AB|}{|AM|} = \frac{a}{d-a} = \frac{|MC|}{|MA|} = \tau$$

が得られる．

もっとわかることがある．重心 S と頂点との距離 s について，関係式 $s^2 = \frac{d^2}{\tau+2}$ を証明することは読者に残しておく（BS は対角線 AC を垂直二等分することに注意する）．幾何への寄り道を終わらせるために，今度は上底が正 5 角形の傘を考える．1 つおきの骨（長さは 1）は垂直だから，ピュタゴラスの定理により $d = \sqrt{2}$ となり，それゆえ $s^2 = \frac{2}{\tau+2} = \frac{4}{\sqrt{5}+5}$ となる．だから，ピュタゴラスをもう一度使えば，高さ $h = |OS|$ に対して，述べておいた結果

$$h^2 \; = \; 1 - s^2 \; = \; \frac{1+\sqrt{5}}{\sqrt{5}+5} \; = \; \frac{1}{\sqrt{5}}$$

が得られる．

さて，とくに「よい」正規直交表現を持つ任意のグラフ G のシャノン容量に対する上界「$\Theta(G) \le \sigma_T^{-1}$」を考えることにしよう．このために $T = \{\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)}\}$ を G の $\mathbb{R}^s$ における正規直交表現とする．ここで，$\boldsymbol{v}^{(i)}$ は頂点 v_i に対応している．さらに，すべてのベクトル $\boldsymbol{v}^{(i)}$ はベクトル $\boldsymbol{u} = \frac{1}{m}(\boldsymbol{v}^{(1)} + \cdots + \boldsymbol{v}^{(m)})$ と同じ角を持つこと，または同じことだが，内積

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle \;=\; \sigma_T$$

がすべての i に対して同じ値 $\sigma_T \neq 0$ を持つことを仮定する．この値 σ_T を表現 T の**定数**と呼ぼう．C_5 を表現するロヴァースの傘に対しては，条件 $\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle = \sigma_T$ は $\boldsymbol{u} = \vec{OS}$ に対して確かに成り立っている．

さて，3 段階に分けて進むことにする．

(A) V 上の確率分布 $\boldsymbol{x} = (x_1, \ldots, x_m)$ を考え，

$$\mu(\boldsymbol{x}) \;=\; |x_1\boldsymbol{v}^{(1)} + \cdots + x_m\boldsymbol{v}^{(m)}|^2,$$
$$\mu_T(G) \;=\; \inf_{\boldsymbol{x}} \mu(\boldsymbol{x})$$

とおく．U を G における最大の独立集合とし（$|U| = \alpha$ とする），$\boldsymbol{x}_U = (x_1, \ldots, x_m)$ を，$v_i \in U$ ならば $x_i = \frac{1}{\alpha}$ で，そうでなければ $x_i = 0$ として定義する．すべてのベクトル $\boldsymbol{v}^{(i)}$ の長さは 1 で，隣接していない任意の 2 つのベクトルに対しては $\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(j)} \rangle = 0$ であるので，

$$\mu_T(G) \;\le\; \mu(\boldsymbol{x}_U) \;=\; \Big|\sum_{i=1}^{m} x_i \boldsymbol{v}^{(i)}\Big|^2 \;=\; \sum_{i=1}^{m} x_i^2 = \alpha\frac{1}{\alpha^2} = \frac{1}{\alpha}$$

となる．こうして $\mu_T(G) \le \alpha^{-1}$ が得られ，したがって

$$\alpha(G) \;\le\; \frac{1}{\mu_T(G)}$$

が得られる．

(B) 次に $\mu_T(G)$ を計算する．ベクトル $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^s$ に対するコーシー–シュヴァルツの不等式

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle^2 \;\le\; |\boldsymbol{a}|^2\,|\boldsymbol{b}|^2$$

が必要となる．$\boldsymbol{a} = x_1\boldsymbol{v}^{(1)} + \cdots + x_m v^{(m)}$ と $\boldsymbol{b} = \boldsymbol{u}$ に適用すると，上の不等式から

$$\langle x_1\boldsymbol{v}^{(1)} + \cdots + x_m\boldsymbol{v}^{(m)}, \boldsymbol{u}\rangle^2 \;\leq\; \mu(\boldsymbol{x})\,|\boldsymbol{u}|^2 \tag{5}$$

が得られる．すべての i に対して $\langle v^{(i)}, \boldsymbol{u}\rangle = \sigma_T$ という仮定から，どんな分布 $\boldsymbol{x}$ に対しても

$$\langle x_1\boldsymbol{v}^{(1)} + \cdots + x_m\boldsymbol{v}^{(m)}, \boldsymbol{u}\rangle \;=\; (x_1 + \cdots + x_m)\,\sigma_T \;=\; \sigma_T$$

となる．こうしてこれは特に，一様分布 $(\frac{1}{m}, \ldots, \frac{1}{m})$ に対しても成り立たねばならない．この分布では $|\boldsymbol{u}|^2 = \sigma_T$ となっている．それゆえ (5) は

$$\sigma_T^2 \;\leq\; \mu(\boldsymbol{x})\,\sigma_T \qquad \text{つまり} \qquad \mu_T(G) \;\geq\; \sigma_T$$

となる．一方，$\boldsymbol{x} = (\frac{1}{m}, \ldots, \frac{1}{m})$ に対しては

$$\mu_T(G) \;\leq\; \mu(\boldsymbol{x}) \;=\; |\tfrac{1}{m}(\boldsymbol{v}^{(1)} + \cdots + \boldsymbol{v}^{(m)})|^2 \;=\; |\boldsymbol{u}|^2 \;=\; \sigma_T$$

となるので，

$$\mu_T(G) \;=\; \sigma_T \tag{6}$$

が証明されたことになる．まとめると，定数 σ_T を持つどんな正規直交表現 T に対しても

$$\alpha(G) \;\leq\; \frac{1}{\sigma_T} \tag{7}$$

という不等式が成り立つことになった．

(C) この不等式を $\Theta(G)$ に拡張するために前と同じようにする．また，2 つのグラフの積 $G \times H$ を考える．G と H はそれぞれ，$\mathbb{R}^r$ と $\mathbb{R}^s$ の中で正規直交表現 R と S を持つとし，定数を σ_R と σ_S とする．$\boldsymbol{v} = (v_1, \ldots, v_r)$ を R の中のベクトル，$\boldsymbol{w} = (w_1, \ldots, w_s)$ を S の中のベクトルとする．対 $(\boldsymbol{v}, \boldsymbol{w})$ に対応する $G \times H$ の頂点に対して，ベクトル

$$\boldsymbol{v}\boldsymbol{w}^T = (v_1w_1, \ldots, v_1w_s, v_2w_1, \ldots, v_2w_s, \ldots, v_rw_1, \ldots, v_rw_s) \in \mathbb{R}^{rs}$$

を対応させる[1]. $R \times S = \{\boldsymbol{v}\boldsymbol{w}^T : \boldsymbol{v} \in R, \boldsymbol{w} \in S\}$ が $G \times H$ の正規直交表現で，定数が $\sigma_R\sigma_S$ であることは直ちに確かめられる．それゆえ (6) から

$$\mu_{R\times S}(G \times H) \;=\; \mu_R(G)\mu_S(H)$$

が得られる．このことから，$G^n = G \times \cdots \times G$ と，定数 σ_T を持つ表現 T に対して，

$$\mu_{T^n}(G^n) \;=\; \mu_T(G)^n \;=\; \sigma_T^n$$

が得られ，(7) から

$$\alpha(G^n) \;\le\; \sigma_T^{-n}, \qquad \sqrt[n]{\alpha(G^n)} \;\le\; \sigma_T^{-1}$$

が得られる．

すべてのことを合わせると，ロヴァースの議論が完成したことになる．

定理． $T = \{\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)}\}$ **が，** G **の正規直交表現で定数が** σ_T**，であれば，次の不等式が成り立つ．**

$$\Theta(G) \;\le\; \frac{1}{\sigma_T}. \tag{8}$$



「骨が 5 つの傘」

ロヴァースの傘を見ると $\boldsymbol{u} = (0, 0, h{=}\frac{1}{\sqrt[4]{5}})^T$ であることがわかり，それゆえ $\sigma = \langle \boldsymbol{v}^{(i)}, \boldsymbol{u}\rangle = h^2 = \frac{1}{\sqrt{5}}$ となり，これから $\Theta(C_5) \le \sqrt{5}$ が得られる．こうしてシャノンの問題が解決したのである．

もう少し議論を先に進めよう．(8) から，G の表現に対して σ_T が大きいほど，$\Theta(G)$ に対するよい限界が得られることになる．どんなグラフ G に対しても正規直交表現を与える方法がある．$G = (V, E)$ に，以下のように定義される**隣接行列** $A = (a_{ij})$ を対応させる．$V = \{v_1, \ldots, v_m\}$ とするとき，

---

[1]　［訳註］普通の線形代数では $\boldsymbol{v}^T\boldsymbol{w}$ が $r \times s$ 行列で，それを $\mathbb{R}^{rs}$ のベクトルと同一視することになり，$\boldsymbol{v}\boldsymbol{w}^T$ では内積になってしまう．ここでは行列の積ではなく，$\boldsymbol{v}\boldsymbol{w}^T$ 自体で 1 つのベクトルを表わしていると考えておくことにしよう．

$$a_{ij} = \begin{cases} 1 & v_iv_j \in E \text{ のとき} \\ 0 & \text{それ以外のとき} \end{cases}$$

とおく．A は実対称行列で，主対角成分は 0 である．

ここで線形代数の 2 つの事実が必要となる．1 つ目は，対称行列として，A は m 個の実固有値 $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m$ を持ち（そのうちのいくつかは等しいかも知れない），固有値の和は A の対角成分の和であり，今は 0 である．それゆえ，(G が辺を持たないという自明な場合を除いて）最小の固有値は負でなければならない．$p = |\lambda_m| = -\lambda_m$ を最小の固有値の絶対値とし，行列

$$M = I + \frac{1}{p}A$$

を考える．ここで，I は $(m \times m)$ 単位行列を表わす．この M の固有値は $1 + \frac{\lambda_1}{p} \geq 1 + \frac{\lambda_2}{p} \geq \cdots \geq 1 + \frac{\lambda_m}{p} = 0$ となる．ここで 2 つ目の結果（線形代数の主軸定理）を述べよう．$M = (m_{ij})$ が実対称行列で，すべての固有値が ≥ 0 であれば，$s = \text{rank}(M)$ として，

$$m_{ij} = \langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(j)} \rangle \qquad (1 \leq i, j \leq m)$$

を満たすベクトル $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)} \in \mathbb{R}^s$ が存在する，というものである．とくに，$M = I + \frac{1}{p}A$ に対しては，

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(i)} \rangle = m_{ii} = 1 \qquad (\text{すべての } i \text{ に対して})$$

かつ

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(j)} \rangle = \frac{1}{p}a_{ij} \qquad (i \neq j \text{ のとき})$$

が得られる．$v_iv_j \notin E$ である限り $a_{ij} = 0$ となるから，ベクトル $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)}$ は実際 G の正規直交表現をなすことがわかる．

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

5 サイクル C_5 に対する隣接行列．

最後に，この構成を，奇数 $m \geq 5$ のときの m サイクル C_m に対して適用してみよう．ここで容易な計算で $p = |\lambda_{\min}| = 2\cos\frac{\pi}{m}$ が得られる（以下の箱を参照のこと）．隣接行列の各行には 2 つの 1 が含まれ，これから行列 M の各行の和が $1 + \frac{2}{p}$ であることがわかる．表現 $\{\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)}\}$ に対して，これは

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(1)} + \cdots + \boldsymbol{v}^{(m)} \rangle = 1 + \frac{2}{p} = 1 + \frac{1}{\cos\frac{\pi}{m}}$$

C_m の固有値

サイクル C_m の隣接行列 A を見る．固有値（と固有ベクトル）を見つけるために，1 の m 乗根を使う．これらは，$\zeta = e^{\frac{2\pi i}{m}}$ とおくとき，$1, \zeta, \zeta^2, \ldots, \zeta^{m-1}$ によって与えられる（38 ページの箱を参照）．$\lambda = \zeta^k$ をこれらの根のうちの 1 つとすれば，$(1, \lambda, \lambda^2, \ldots, \lambda^{m-1})^T$ は固有値 $\lambda + \lambda^{-1}$ に属する A の固有ベクトルであることを言おう．実際，A の構成によって

$$A\begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{m-1} \end{pmatrix} = \begin{pmatrix} \lambda & + & \lambda^{m-1} \\ \lambda^2 & + & 1 \\ \lambda^3 & + & \lambda \\ & \vdots & \\ 1 & + & \lambda^{m-2} \end{pmatrix} = (\lambda + \lambda^{-1})\begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{m-1} \end{pmatrix}$$

であることがわかる．ベクトル $(1, \lambda, \ldots, \lambda^{m-1})$ は独立だから（それらはいわゆるヴァンデルモンドの行列をなす），奇数の m に対して

$$\begin{aligned} \zeta^k + \zeta^{-k} &= [(\cos(2k\pi/m) + i\sin(2k\pi/m)] \\ &\quad + [\cos(2k\pi/m) - i\sin(2k\pi/m)] \\ &= 2\cos(2k\pi/m) \qquad (0 \le k \le \tfrac{m-1}{2}) \end{aligned}$$

がすべて A の固有値であるという結論になる．さて，コサインは減少関数なので，

$$2\cos\left(\frac{(m-1)\pi}{m}\right) = -2\cos\frac{\pi}{m}$$

が A の最小の固有値となる．

を意味しており，それゆえ，すべての i に対して，

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle = \frac{1}{m}(1 + (\cos\tfrac{\pi}{m})^{-1}) = \sigma$$

となる．したがって，主結果 (8) を適用することができ，

$$\Theta(C_m) \le \frac{m}{1+(\cos\frac{\pi}{m})^{-1}} \qquad (\text{奇数}\, m \ge 5\, \text{に対して}) \qquad (9)$$

と結論される．

$\cos\frac{\pi}{m} < 1$ だから，限界 (9) は，前に発見した限界 $\Theta(C_m) \le \frac{m}{2}$ よりもよいことに注意する．さらに，$\cos\frac{\pi}{5} = \frac{\tau}{2}$ となる．ここで，$\tau = \frac{\sqrt{5}+1}{2}$ は黄金比である．それゆえ $m=5$ に対しては，また

$$\Theta(C_5) \le \frac{5}{1+\frac{4}{\sqrt{5}+1}} = \frac{5(\sqrt{5}+1)}{5+\sqrt{5}} = \sqrt{5}$$

が得られる．この構成で与えられる正規直交表現は，もちろん，「ロヴァースの傘」そのものである．

さらに，C_7, C_9 や他の奇数サイクルについてはどうなっているのだろうか？ $\alpha(C_m^2)$, $\alpha(C_m^3)$ や他の小さいベキを考えることによって，下界 $\frac{m-1}{2} \le \Theta(C_m)$ は確かに大きくなる可能性があるが，どんな奇数の $m \ge 7$ に対しても，知られている最良の下界が (8) で与えられる上界に一致することはない．だから，ロヴァースの $\Theta(C_5) = \sqrt{5}$ の素晴らしい証明から 20 年経ったが，これらの問題は未解決のままであり，非常に難しいと考えられている．しかし，結局のところ，こんな状況(こと)は前にもあったことである．

たとえば，$m=7$ のとき，わかっているのは

$$\sqrt[5]{343} \le \Theta(C_7) \le \frac{7}{1+(\cos\frac{\pi}{7})^{-1}}$$

ということだけである．これは大体 $3.2141 \le \Theta(C_7) \le 3.3177$ である．

参考文献

[1] V. ホヴァタル：『線形プログラミング』(*Linear Programming*), Freeman, New York 1983.

[2] W. ヒーマーズ：「固有値の方法」(*Eigenvalue methods*), 『組合せ論におけるパッキングと被覆』(Packing and Covering in Combinatorics), A. Schrijver, ed., Math. Centre Tracts **106** (1979), 15-38.

[3] L. ロヴァース：「グラフのシャノン容量について」(*On the Shannon capacity of a graph*), IEEE Trans. Information Theory **25** (1979), 1-7.

[4] C. E. シャノン：「雑音のあるチャンネルの誤りゼロ容量」(*The zero-error capacity of a noisy channel*), IRE Trans. Information Theory **3** (1956), 3-15.

第31章　友人と政治家について

誰が最初に次の問題を提案したか，もしくは誰が問題に人間的なタッチを与えたかは知られていない．

ある人間の集団があって，その中の任意の2人の人にちょうど1人の共通の友人があると仮定する．そのとき，あらゆる人の友人であるような人（「政治家」）が常に存在する．

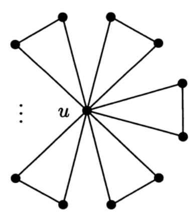


「政治家の微笑」

数学者の言葉では，**友情定理**と呼ばれている．

証明に取り掛かる前に，グラフ理論の言葉で問題を言い換えておこう．人々を頂点の集合 V と解釈し，2つの頂点が辺で結ばれるのを対応する人々が友人であるときとする．暗黙の了解として，友情は常に双方向のものとする．つまり，u が v の友人なら，v も u の友人とする．さらに，誰も，彼もしくは彼女自身の友人ではないとする．すると，問題は次の形になる．

定理． G **を有限グラフとし，** G **の任意の2つの頂点はちょうど1つの共通の頂点と隣接しているとする．そのとき，他のすべての頂点と隣接する頂点が存在する．**



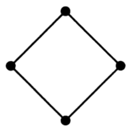
風車グラフ．

無限グラフに対しては定理が成り立たないことに注意する．たとえば，5サイクルから始めて，まだ共通の隣接頂点を持っていないすべての頂点対に，新しい隣接頂点をグラフに追加することを繰り返す．すると，政治家を持たない（可算）無限の友情グラフが得られる．

図にあるようにこの性質を持つグラフが存在することに注意する．そこでは u が政治家である．実際，このような「風車グラフ」がこの性質

を持つ唯一のグラフであるを示すことになる．

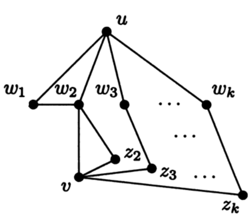
政治家がいてこそ風車グラフが存在し得るのは，明らかだろう．友情定理の証明はいくつか存在するが，ポール・エルデシュ，アルフレッド・レニイ，ヴェラ・ソスによって与えられた最初の証明が今でも一番の完成品である．



■ **証明．** 主張が間違っていて，G が反例になっているとする．つまり，G のどの頂点も他のすべての頂点とは隣接してはいないとする．矛盾を導くのに 2 段階で行う．最初の部分は組合せ論で，第 2 の部分は線形代数である．

(1) G が正則グラフになる，つまり，どんな $u, v \in V$ に対しても $d(u) = d(v)$ であることを示そう．最初に，定理の条件から，G には長さ 4 のサイクルが存在し得ないことに注意する．このことを C_4 **条件**と呼ぶことにする．

最初に，任意の 2 つの**隣接**していない頂点 u と v が同じ次数 $d(u) = d(v)$ を持つことを証明する．$d(u) = k$ とし，$w_1, \ldots, w_k$ が u に隣接しているとする．w_i のうちのただ 1 つが v に隣接しており，それを w_2 とする．w_2 は他の w_i のうちのただ 1 つと隣接していて，それを w_1 とすると，余白の図のような状況になっている．頂点 v は，w_1 とは共通に w_2 と隣接しており，また w_i $(i \geq 2)$ との共通の隣接頂点は z_i $(i \geq 2)$ となっている．C_4 条件からこれらの z_i はすべて異なっていなければならない．これから $d(v) \geq k = d(u)$ が結論され，さらに対称性から $d(u) = d(v) = k$ がわかる．



(1) の証明を終えよう．w_2 以外のどんな頂点も u か v のいずれかとは隣接せず，それゆえ，すでに証明したことから次数 k を持つことがわかる．しかし，w_2 もまた隣接しない頂点を持つので，これも次数 k を持つことになり，よって G は k 正則である．

u の k 個の隣接頂点の次数を足し合わせれば，k^2 となる．(u 以外の) あらゆる頂点は u とちょうど 1 つの共通の隣接頂点を持つから，u 以外の頂点を数え上げたことになり，u については k 回数えたことになる．だから，G の頂点全体の数は

$$n = k^2 - k + 1 \tag{1}$$

となる．

(2) 証明の残りは，線形代数のある標準的な結果の美しい応用になっている．まず，k は 2 より大きくないといけないことに注意する．なぜなら，$k \leq 2$ に対しては，式 (1) から $G = K_1$ と $G = K_3$ だけが起こり得るが，両方とも自明な風車グラフであるからである．278 ページで定義した隣接行列 $A = (a_{ij})$ を考える．(1) から，どんな行にも k 個の 1 があり，定理の条件からどの 2 つの行に対しても，ともに 1 になる列がちょうど 1 つある．さらに，主対角線は 0 になっていることに注意する．それゆえ，

$$A^2 = \begin{pmatrix} k & 1 & \cdots & 1 \\ 1 & k & & 1 \\ \vdots & & \ddots & \vdots \\ 1 & \cdots & 1 & k \end{pmatrix} = (k-1)I + J$$

となる．ここで，I は単位行列で，J はすべての成分が 1 の行列である．J の固有値が（重複度 1 の）n と（重複度 $n-1$ の）0 であることは容易に確かめられる．これから，A^2 の固有値が（重複度 1 の）$k-1+n = k^2$ と（重複度 $n-1$ の）$k-1$ となる．

A は対称行列で，それゆえ対角化可能だから，A の固有値は（重複度 1 の）k [1]と $\pm\sqrt{k-1}$ とになる．r 個の固有値が $\sqrt{k-1}$ で，s 個の固有値が $-\sqrt{k-1}$ であるとする．ただし，$r + s = n - 1$ である．さてあとはもうほんの少しである．A の固有値の和はトレース（今は 0 になっている）だから，

$$k + r\sqrt{k-1} - s\sqrt{k-1} = 0$$

となり，とくに $r \neq s$ であり，

$$\sqrt{k-1} = \frac{k}{s-r}$$

となる．これから $\sqrt{k-1}$ は整数 h となり（$\sqrt{m}$ が有理数なら整数になる！），

$$h(s-r) = k = h^2 + 1$$

[1] ［訳註］k が A の固有値であることは，198 ページと同じ議論でわかる．

が得られる．h が h^2+1 と h^2 を割り切るので，h は 1 とならねばならず，$k=2$ となるのだが，これはすでに除外した値である．こうして矛盾にぶつかったので，証明は終わる．　□

しかし，話は全く終わりというわけではない．定理を「グラフ G が，その任意の 2 頂点の間に長さ 2 の道がちょうど 1 つあるという性質を満たすとする」と言い換えてみよう．明らかに，これは友情定理の条件と同値な定式化である．すると，定理によってこのようなグラフは風車グラフしかないことになる．しかし，2 より長い道を考えたらどうなるだろうか？ アントン・コツィヒの予想は，類似の状況が不可能であるというものである．

コツィヒの予想． **$\ell > 2$ とする．そのとき，その任意の 2 頂点の間に長さ ℓ の道がちょうど 1 つあるという性質を満たすグラフは存在しない．**

コツィヒ自身は $\ell \leq 8$ に対して予想を証明した．[3] において，彼の予想は $\ell = 20$ まで証明され，またすべての $\ell \leq 33$ に対して証明したと最近 A. コストチカが話してくれた．しかし，一般の証明は我々の手の届く範囲にはないように見える．

参考文献

[1] P. エルデシュ，A. レニイ，V. ソス：「グラフ理論のある問題について」(*On a problem of graph theory*), Studia Sci. Math. **1** (1966), 215-235.

[2] A. コツィヒ：「正則 k 弧状連結グラフ」(*Regularly k-path connected graphs*), Congressus Numerantium **40** (1983), 137-141.

[3] A. コストチカ：「ある一般友情グラフの非存在について」(*The nonexistence of certain generalized friendship graphs*), “Combinatorics” (Eger, 1987), Colloq. Math. Soc. János Bolyai **52**, North-Holland, Amsterdam 1988, 341-356.

第32章　確率は（ときに）数え易くする

本書を数論におけるポール・エルデシュの初期の論文から始めたのと同じように，本書を締めくくるのもおそらくは彼のもっとも永く続く伝説になると考えられるものにしよう．それはアルフレッド・レニイとともに行った**確率的方法**の導入である．一番単純には次のように述べられる．

> **与えられた対象の集合の中で，対象がある性質を持たない確率が1より小さければ，この性質を持つ対象は存在しなければならない．**

こうして**存在**を示す結果が得られる．この対象を見つけることは非常に難しいかも知れないが（またそういうことが多いのだが），存在することはわかるのである．ここで，この確率的方法のエルデシュによる3つの例を（易しいものから順に）述べていき，とくにエレガントな真新しい応用で締めくくることにする．

小手調べとして，ある有限の基礎集合 X の部分集合 A_i の族 $\mathcal{F}$ で，すべてのサイズが $d \geq 2$ であるものを考える．$\mathcal{F}$ が **2 彩色可能**であるというのは，2 色による X の彩色で，あらゆる集合 A_i の中に両方の色が現れるものが存在するときとする．あらゆる族がこのように彩色可能であるわけではないことは直ちにわかる．その例としては，$(2d-1)$ 集合 X のサイズ d のすべての部分集合をとる．すると，どのように X を 2 色で塗ったとしても，同じ色で塗られた d 個の元がなければならない．一方，d 集合の 2 彩色可能な族のあらゆる部分族はそれ自身 2 彩色可能であることも同じように明らかである．それゆえ，2 彩色可能でない $m = m(d)$ 個の集合の族が存在するような**最小**の数に興味が持たれ

る．言い換えてみると，$m(d)$ は，$m(d)$ 個より少ない集合のなすあらゆる族が2彩色可能であることを保証する最小の数である．

定理 1. **高々 2^{d-1} 個の d 集合のなすあらゆる族は2彩色可能である．つまり $m(d) > 2^{d-1}$ である．**

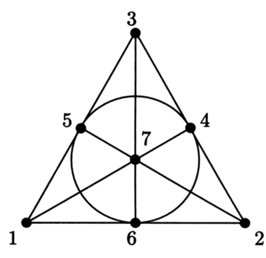
■ **証明.** $\mathcal{F}$ を高々 2^{d-1} 個の d 集合のなす族とする．X を2色で，すべての彩色が同等に確からしいように，ランダムに彩色する．各集合 $A \in \mathcal{F}$ に対し，E_A を A のすべての元が同じように彩色されるという事象とする．そのような彩色はちょうど2つあるので，

$$\mathrm{Prob}(E_A) \quad = \quad \left(\tfrac{1}{2}\right)^{d-1}$$

となり，それゆえ $m = |\mathcal{F}| \le 2^{d-1}$ としたとき（E_A たちが排反事象でないことに注意する），

$$\mathrm{Prob}\Big(\bigcup_{A\in\mathcal{F}} E_A\Big) \quad < \quad \sum_{A\in\mathcal{F}} \mathrm{Prob}(E_A) \quad = \quad m\left(\tfrac{1}{2}\right)^{d-1} \quad \le \quad 1$$

となる．X の2彩色で，1色で塗られる集合を持たないものが存在するという結論が得られるが，これが我々の2彩色可能性の条件であった．　□



$m(d)$ の上界は大雑把には $d^2 2^d$ で，それもエルデシュによって求められた．これもまた確率的方法を使うのだが，今度はランダムな集合と固定した彩色を使う．厳密な値が知られているのは最初の2つだけで，$m(2) = 3$ と $m(3) = 7$ である．もちろん，$m(2) = 3$ はグラフ K_3 によって実現され，一方ファノの配置によって $m(3) \le 7$ がわかる．ここで，$\mathcal{F}$ は図の（円周の集合 $\{4,5,6\}$ を含んだ）7つの3集合からなる．$\mathcal{F}$ には3色が必要であることを示すのは読者には面白い問題になるだろう．6つの3集合からなるどんな族も2彩色可能であること，それゆえ $m(3) = 7$ であることを証明するには，さらにちょっとした注意が必要である．

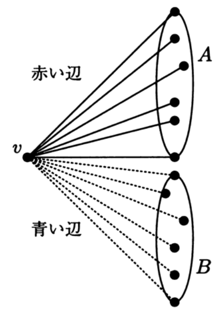
次に述べる例はこの分野の古典である，ラムゼイ数である．N 個の頂点上の完全グラフ K_N を考える．K_N が性質 (m,n) を持つというのを，K_N の辺にどのように赤と青で色を塗ろうとも，すべての辺が赤で塗られている m 個の頂点上の完全部分グラフか，すべての辺が青で塗られている n 個の頂点上の完全部分グラフのどちらかが常に存在するときとする．K_N が性質 (m,n) を持てば，$s \ge N$ に対するあらゆる K_s も同

じ性質を持つことは明らかである．だから，最初の例と同じように，（もし存在するなら）この性質を持つ最小の数 N を求めよう．この数が**ラムゼイ数** $R(m,n)$ である．

初めに，$R(m,2)=m$ となるのは確かである．なぜなら，K_m のすべての辺が赤で塗られているか，青の辺があるかであるが，あとの場合には青の K_2 が存在するからである．対称性により，$R(2,n)=n$ が得られる．さて，$R(m-1,n)$ と $R(m,n-1)$ が存在すると仮定しよう．そのとき，$R(m,n)$ が存在し，

$$R(m,n) \quad \leq \quad R(m-1,n) \ + \ R(m,n-1) \tag{1}$$

となることを証明する．$N=R(m-1,n)+R(m,n-1)$ とし，K_N に任意に赤と青の色を塗ったとしよう．頂点 v に対し，v と赤い辺で結ばれた頂点の集合を A，青い辺で結ばれた頂点の集合を B とする．



$|A|+|B|=N-1$ だから，$|A|\geq R(m-1,n)$ か $|B|\geq R(m,n-1)$ のどちらかが成り立つ．$|A|\geq R(m-1,n)$ としよう．もう1つの場合は同様である．すると，$R(m-1,n)$ の定義から，A の中にすべての辺が赤く塗られているサイズが $m-1$ の部分集合 A_R が存在し，v と合わせて赤い K_m が存在するか，もしくはすべての辺が青く塗られているサイズ n の部分集合 A_B が存在することになる．K_N が性質 (m,n) を持つことがわかり，主張 (1) が得られる．

(1) と初めの値 $R(m,2)=m$ と $R(2,n)=n$ とを合わせると，2項係数のよく知られた漸化式から

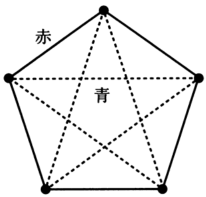
$$R(m,n) \quad \leq \quad \binom{m+n-2}{m-1}$$

が得られ，とくに

$$R(k,k) \ \leq \ \binom{2k-2}{k-1} = \binom{2k-3}{k-1} + \binom{2k-3}{k-2} \leq 2^{2k-3} \tag{2}$$

が得られる．

こうして，本当に興味があるのは $R(k,k)$ に対する下界ということになる．このためには，あらゆる $N<R(k,k)$ に対して，どんな部分 K_k にも赤だけとか青だけの色のものが存在しないような，辺の色彩が**存在する**ことを証明することになる．そして，ここが確率的方法の出番なのである．



定理 2. **すべての $k \geq 2$ に対して，ラムゼイ数に対する下からの評価**

$$R(k,k) \quad \geq \quad 2^{\frac{k}{2}}$$

が成り立つ．

■ **証明.** $R(2,2)=2$ はわかっている．(2) から $R(3,3) \leq 6$ であることはわかっているが，図の 5 角形から，$R(3,3)=6$ がわかる．

さて，$k \geq 4$ と仮定しよう．$N < 2^{\frac{k}{2}}$ であると仮定し，すべての赤–青彩色を考え，各辺を赤と青で塗るのは独立で確率 $\frac{1}{2}$ であるとする．こうするとすべての彩色は確率 $2^{-\binom{N}{2}}$ で同じ程度の確からしいことになる．A をサイズ k の頂点集合とすると，A の辺がすべて赤く塗られる事象 A_R の確率は $2^{-\binom{k}{2}}$ となる．それゆえ，ある k 集合に対してすべてが赤く塗られるという確率 p_R は

$$p_R \quad = \quad \text{Prob}\Big(\bigcup_{|A|=k} A_R\Big) \quad \leq \quad \sum_{|A|=k} \text{Prob}(A_R) \quad = \quad \binom{N}{k} 2^{-\binom{k}{2}}$$

で抑えられる．

さて，$N < 2^{\frac{k}{2}}$ かつ $k \geq 4$ だから，$k \geq 2$ に対して $\binom{N}{k} \leq \frac{N^k}{2^{k-1}}$ であること（16 ページ参照）を使うと，

$$\binom{N}{k} 2^{-\binom{k}{2}} \ \leq \ \frac{N^k}{2^{k-1}} 2^{-\binom{k}{2}} \ < \ 2^{\frac{k^2}{2}-\binom{k}{2}-k+1} \ = \ 2^{-\frac{k}{2}+1} \leq \frac{1}{2}$$

が得られる．それゆえ $p_R < \frac{1}{2}$ となり，対称性から $p_B < \frac{1}{2}$ となる．ただし，p_B は，そのすべての辺が青で塗られるような k 個の頂点集合があるための確率である．これから，$N < 2^{\frac{k}{2}}$ に対して $p_R + p_B < 1$ という結論が得られ，だから全部赤か青かの K_k が存在しないような彩色が存在しなければならず，つまり，K_N は性質 (k,k) を持たないことになる． □

もちろん，$R(k,k)$ に対する下界と上界の間にはかなりのギャップがある．エルデシュの結果から 50 年以上が経ってもなお，この天書の証明ほど簡明な，一般の k に対する，よりよい指数を持つ下界は得られていない．実際，ある固定した $\varepsilon > 0$ に対して，$R(k,k) > 2^{(\frac{1}{2}+\varepsilon)k}$ の形の下界も $R(k,k) < 2^{(2-\varepsilon)k}$ の形の上界も見つけた者はいない．

3 つ目の結果は，確率的方法のもう 1 つの美しい説明になっている．n

個の頂点の上のグラフ G とその彩色数 $\chi(G)$ を考える．もし $\chi(G)$ が大きい，つまり，多くの色が必要であれば，G がある大きな完全グラフを含むように思うかも知れない．しかし，これは真実からほど遠いのである．1940 年代に，すでにブランシュ・デカルトは，任意に大きい彩色数を持ち，三角形を含まない，つまりあらゆるサイクルが少なくとも長さ 4 のグラフを構成している（次ページの箱を参照）．また何人かの人も同じことをしている．

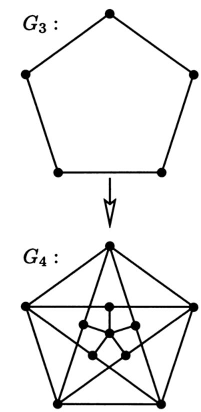
しかし，これらの例では長さ 4 のサイクルをたくさん含んでいる．もっとよくすることはできるだろうか？ 小さい長さのサイクルを持たず，任意に大きい彩色数を持つことが要求できるだろうか？ それができるのである！ きちんと述べるために，G における最小のサイクルの長さを G の**周寸** $\gamma(G)$ と呼ぶと，次の定理が得られる．これも，エルデシュが最初に証明をした．

定理 3. あらゆる $k \geq 2$ に対して，彩色数が $\chi(G) > k$ で，周寸が $\gamma(G) > k$ のグラフ G が存在する．

戦略は前の証明と似ている．グラフの上のある確率空間を考え，$\chi(G) \leq k$ に対する確率が $\frac{1}{2}$ より小さく，同じように $\gamma(G) \leq k$ に対する確率が $\frac{1}{2}$ より小さいことを示すというように進む．その結果，欲しい性質を持つグラフが存在しなければならなくなる．

■ **証明.** $V = \{v_1, v_2, \ldots, v_n\}$ を頂点の集合とし，p を 0 と 1 の間の固定した数とする．ただし，p はあとで慎重に選ぶことになる．考える確率空間 $\mathcal{G}(n,p)$ は，V 上のすべてのグラフからなり，個々の辺は確率 p で互いに独立に現れるとする．言い換えれば，各辺に対し確率 p で（表が出るコインを）投げるベルヌーイ試行になっている．たとえば，完全グラフに対する確率 $\mathrm{Prob}(K_n)$ は $\mathrm{Prob}(K_n) = p^{\binom{n}{2}}$ である．一般に，V 上のグラフ H がちょうど m 個の辺を持っていれば，$\mathrm{Prob}(H) = p^m(1-p)^{\binom{n}{2}-m}$ となる．

まず彩色数 $\chi(G)$ を見てみよう．**独立数**，つまり，G における最大の独立集合のサイズを $\alpha = \alpha(G)$ と表わす．$\chi = \chi(G)$ 種の色を使った彩色ではすべての色の類は独立（それゆえサイズは $\leq \alpha$）なので，$\chi\alpha \geq n$ となる．したがって，α が n に比べて小さければ，χ は大きくないといけないことになり，それが欲しかったことである．



ミチエルスキ・グラフの構成.

大きな彩色数の，三角形のないグラフ

三角形を持たず，

$$\chi(G_n) = n$$

を満たすグラフの列 $G_3, G_4, \ldots$ がある．5 サイクル $G_3 = C_5$ として始めよう．$\chi(G_3) = 3$ となっている．すでに G_n が構成されていて，その頂点集合を V とする．その次のグラフ G_{n+1} の頂点集合は $V \cup V' \cup \{z\}$ で，頂点 $v' \in V'$ は $v \in V$ と 1 対 1 に対応しており，z はそれら以外の 1 つの頂点である．G_{n+1} の辺は 3 種類に分かれる．まず，G_n のすべての辺をとり，次に，あらゆる頂点 v' を G_n における v の隣接頂点と結び，最後に z をすべての $v' \in V'$ と結ぶ．それゆえ，$G_3 = C_5$ から G_4 として得られるものがいわゆる**ミチエルスキ・グラフ**である．

明らかに，G_{n+1} はまた三角形を持たない．$\chi(G_{n+1}) = n+1$ を証明するために，n についての帰納法を使う．G_n の任意の n 彩色をとり，色の類を C とする．頂点 $v \in C$ で，あらゆる他の色の類の少なくとも 1 つの頂点と隣接しているものが存在しなければならない．もしそうでなければ，C の頂点を他の $n-1$ 種の色の類に分配することができて，$\chi(G_n) \le n-1$ となってしまうからである．しかし今，明らかに（v に対応する V' の頂点である）v' は，この n 彩色での v と同じ色をとらねばならない．だから，n 種の色はすべて V' の中に現れており，z に対しては新しい色が必要となる．

$2 \le r \le n$ とする．V におけるある固定した r 集合が独立であるための確率は $(1-p)^{\binom{r}{2}}$ であり，定理 2 と同じ議論によって，

$$\begin{aligned}\text{Prob}(\alpha \ge r) &\le \binom{n}{r}(1-p)^{\binom{r}{2}} \le n^r(1-p)^{\binom{r}{2}} \\ &= (n(1-p)^{\frac{r-1}{2}})^r \ \le\ (ne^{-p(r-1)/2})^r\end{aligned}$$

を得ることができる．なぜなら，すべての p に対して，$1-p \leq e^{-p}$ だからである．

任意の $k>0$ を固定したとき，$p=n^{-\frac{k}{k+1}}$ と選び，十分大きな n に対して

$$\mathrm{Prob}\Big(\alpha \geq \frac{n}{2k}\Big) \ < \ \frac{1}{2} \tag{3}$$

となることを示すことにする．実際，$n^{\frac{1}{k+1}}$ は $\log n$ より速く増大するので，十分大きな n に対して $n^{\frac{1}{k+1}} \geq 6k\log n$ となり，だから $p \geq 6k\frac{\log n}{n}$ となる．$r=\lceil \frac{n}{2k} \rceil$ に対しては，これから $pr \geq 3\log n$ が得られ，よって

$$ne^{-p(r-1)/2} \ = \ ne^{-\frac{pr}{2}}e^{\frac{p}{2}} \ \leq \ ne^{-\frac{3}{2}\log n}e^{\frac{1}{2}} \ = \ n^{-\frac{1}{2}}e^{\frac{1}{2}} \ = \ (\tfrac{e}{n})^{\frac{1}{2}}$$

となるが，これは，n が無限に大きくなるとき 0 に収束する．それゆえ，(3) はすべての $n \geq n_1$ に対して成り立つ．

今度は第 2 のパラメータ $\gamma(G)$ を見てみよう．k が与えられたときに，長さが $\leq k$ のサイクルがあまり多くないことを示したいのである．i を 3 と k の間の数とし，i 集合 $A \subseteq V$ を 1 つ固定する．A 上の可能な i サイクルの数は，明らかに，A の円順列の数を 2 で割ったものになり（どちらの方向にも廻って行けるから），その数は $\frac{(i-1)!}{2}$ となる．したがって，可能な i サイクル全体の数は $\binom{n}{i}\frac{(i-1)!}{2}$ となり，そのようなサイクル C はどれも確率 p^i で現れる．X を長さ $\leq k$ のサイクルの数を数える確率変数とする．X を評価するために，2 つの単純だが美しい道具を使う．1 つは期待値の線形性で，もう 1 つは，非負の確率変数に対するマルコフの不等式である．それは，EX を X の期待値とするとき，

$$\mathrm{Prob}(X \geq a) \ \leq \ \frac{EX}{a}$$

が成り立つというものである．この 2 つの道具については，第 13 章の附録を参照のこと．

X_C を，あるサイクル C の，たとえば長さを i として，特性確率変数としよう．つまり，グラフの中に C が現れるかどうかに従って $X_C=1$ または 0 とおくのである．それゆえ，$EX_C=p^i$ となる．X は長さが $\leq k$ のすべてのサイクルの数を数えるものだから，$X=\sum X_C$ であり，線形性から，

$$EX \ = \ \sum_{i=3}^{k} \binom{n}{i} \frac{(i-1)!}{2} p^i \ \leq \ \frac{1}{2} \sum_{i=3}^{k} n^i p^i \ \leq \ \frac{1}{2}(k-2) n^k p^k$$

となる．最後の不等式は，$np = n^{\frac{1}{k+1}} \geq 1$ のおかげで成り立つ．$a = \frac{n}{2}$ としてマルコフの不等式を使えば，

$$\mathrm{Prob}(X \geq \tfrac{n}{2}) \ \leq \ \frac{EX}{n/2} \ \leq \ (k-2)\frac{(np)^k}{n} \ = \ (k-2) n^{-\frac{1}{k+1}}$$

が得られる．右辺は，n が無限に大きくなるとき 0 に収束するので，$n \geq n_2$ に対して $p(X \geq \frac{n}{2}) < \frac{1}{2}$ となるだろう．

あともうほんの少しになった．上の解析により，$n \geq \max(n_1, n_2)$ に対して，n 頂点上のグラフ H であって，$\alpha(H) < \frac{n}{2k}$ を満たし，長さ $\leq k$ のサイクルの数が $\frac{n}{2}$ より小さいものが存在する．このサイクルのそれぞれから 1 つの頂点を取り去って得られるグラフを G とする．ともかく $\gamma(G) > k$ ではある．G の頂点数は $\frac{n}{2}$ より多く，$\alpha(G) \leq \alpha(H) < \frac{n}{2k}$ が成り立っているから，

$$\chi(G) \ \geq \ \frac{n/2}{\alpha(G)} \ \geq \ \frac{n}{2\alpha(H)} \ > \ \frac{n}{n/k} \ = \ k$$

が得られ，証明が終わる．　□

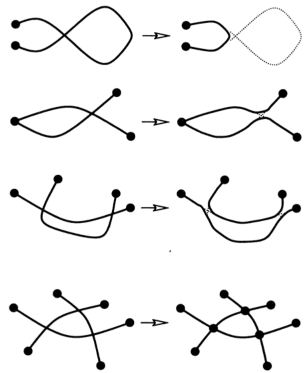
周寸と彩色数が大きな（巨大なサイズの）グラフの具体的な構成は知られている．(対照的に，定理 2 によって存在は与えられている，赤–青彩色で，単色の大きなクリークを持たないものは，どう構成してよいか知られていない.）エルデシュの証明で今も驚くべきなのは，彩色数と周寸が大きな比較的小さなグラフの存在の証明になっていることである．

確率の世界への訪問のお仕舞いに，幾何的なグラフ理論における 1 つの重要な結果（これもポール・エルデシュに遡るが）を述べることにしよう．その魅力的な天書の証明はごく最近得られたものである．

頂点が n 個，辺が m 個の単純グラフ $G(V, E)$ を考える．平面グラフでしたように，G を平面に埋め込みたい．オイラーの公式の結果として，第 10 章で，単純平面グラフ G は高々 $3n-6$ 個の辺しか持たないことがわかっている．それゆえ，m が $3n-6$ より大きければ，辺の交差が起きてしまう．そこで，**交差数** $\mathrm{cr}(G)$ を，G のすべての埋め込みの中での最小の交差数として，自然に定義しよう．すると，$\mathrm{cr}(G) = 0$ であるのは，G が平面グラフのとき，かつそのときに限ることになる．

そのような極小の埋め込みでは，次の3つの状況は排除されている．

- どんな辺も自分自身とは交差しない．
- 共通の端点を持つ辺どうしは交差しない．
- 2つの辺が2度交差することはない．



こうなる理由は，どの場合でも，図で示したような操作を使い，同じグラフを別の描き方で，より少ない交差にすることができるからである．だから，以下では，どんな埋め込みも上の規則を満たしていると仮定する．

G は $\mathbb{R}^2$ に埋め込まれ，交差の数は $\mathrm{cr}(G)$ であるとする．直ちに，交差の数に関する1つの下界を導くことができる．次のグラフ H を考える．H の頂点は，G の頂点にすべての交差点を合わせたものとし，H の辺は，元々の辺の，交差点から交差点までの部分をすべて考えたものである．

すると，新しいグラフ H は平面単純グラフになっている（これは上の3つの仮定からわかる！）．H における頂点の数は $n+\mathrm{cr}(G)$ で，辺の数は $m+2\mathrm{cr}(G)$ である．なぜなら，新しい頂点はすべて次数4だからである．平面グラフに対する辺の数の上界の式を使えば，

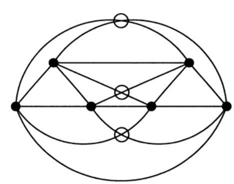
$$m+2\,\mathrm{cr}(G) \quad \leq \quad 3(n+\mathrm{cr}(G))-6$$

が，つまり

$$\mathrm{cr}(G) \quad \geq \quad m-3n+6 \tag{4}$$

が得られる．

たとえば，完全グラフ K_6 に対して計算すると，



$$\mathrm{cr}(K_6) \geq 15-18+6=3$$

となり，実際交差がちょうど3つの埋め込みが存在する．

下界 (4) は，m が n に関して線形のときは十分よいものだが，m が n に比べて大きくなると，様子は変わり，次の定理が成り立つ．

定理 4. **G を単純グラフで，頂点が n 個，辺が m 個とする．ただし，$m \geq 4n$ とする．そのとき**

$$\mathrm{cr}(G) \quad \geq \quad \frac{1}{64}\frac{m^3}{n^2}$$

が成り立つ．

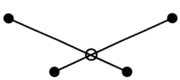
交差補題と呼ばれるこの結果の歴史は，とても面白い．予想をしたのは，エルデシュとガイで，1973 年のことである（$\frac{1}{64}$ ではなくてある定数 c という形だった）．最初に証明したのはレイトンで，1982 年のことであり（$\frac{1}{64}$ ではなく $\frac{1}{100}$ でだった），また独立にアイタイ，ホヴァタル，ニューボーン，セメレディによっても証明された．交差補題はあまり知られてこなかったが（実際，もとの証明が出たあとでも，多くの人々はまだ予想だと思っていた），それはラースロー・ゼケリーがある美しい論文で，それまでは難しいとされてきた幾何的な多様な極値問題に適用することで，交差補題の有用性を示すまでのことであった．今から述べる証明は，ベルナール・シャゼル，ミーシャ・シャリル，エモ・ヴェルズルとの間での電子メールのやり取りから生まれたもので，疑いもなく天書の証明になっている．

■ **証明.** G の極小な埋め込みを考え，p を 0 と 1 の間の数とする（値はあとで決める）．G のあらゆる頂点を独立に確率 p で選び，選ばれた頂点たちによって誘導されるグラフを G_p と書く．

n_p, m_p, X_p をそれぞれ，G_p における頂点，辺，交差の数を数える確率変数とする．どんなグラフに対しても，(4) によって $\mathrm{cr}(G)-m+3n \geq 0$ が成り立つから，期待値に対しても確かに，

$$E(X_p - m_p + 3n_p) \;\geq\; 0$$

となっている．さて，個々の期待値 $E(n_p), E(m_p), E(X_p)$ を計算しよう．明らかに，$E(n_p) = pn$ であり，ある辺が G_p の中に現れるのはその端頂点の両方が G_p の中に現れるのと同値なので，$E(m_p) = p^2 m$ となる．そして最後に $E(X_p) = p^4 \mathrm{cr}(G)$ となる．なぜなら，交差が G_p の中に現れるのは，4 つの（異なる！）頂点がすべてそこに含まれることと同値だからである．



こうして期待値の線形性から

$$0 \;\leq\; E(X_p) \;-\; E(m_p) \;+\; 3E(n_p) \;=\; p^4 \mathrm{cr}(G) - p^2 m + 3pn$$

が得られ，

$$\mathrm{cr}(G) \;\geq\; \frac{p^2 m - 3pn}{p^4} \;=\; \frac{m}{p^2} - \frac{3n}{p^3} \qquad (5)$$

が得られる．ここがサワリである．$p = \frac{4n}{m}$（仮定からこれは高々 1 である）とおけば，(5) は

$$\mathrm{cr}(G) \geq \frac{1}{64}\left[\frac{4m}{(n/m)^2} - \frac{3n}{(n/m)^3}\right] = \frac{1}{64}\frac{m^3}{n^2}$$

となる．これで終わり．□

ポール・エルデシュは，この証明を見たらきっと喜ぶだろう．

参考文献

[1] M. アイタイ，V. ホヴァタル，M. ニューボーン，E. セメレディ：「交差のない部分グラフ」(*Crossing-free subgraphs*), Annals of Discrete Mathematics **12** (1982), 9-12.

[2] N. アロン，J. スペンサー：『確率的方法』(*The Probabilistic Method*), Wiley-Interscience 1992.

[3] P. エルデシュ：「グラフ理論におけるいくつかの注意」(*Some remarks on the theory of graphs*), Bulletin Amer. Math. Soc. **53** (1947), 292-294.

[4] P. エルデシュ：「グラフ理論と確率」(*Graph theory and probability*), Canadian J. Math. **11** (1959), 34-38.

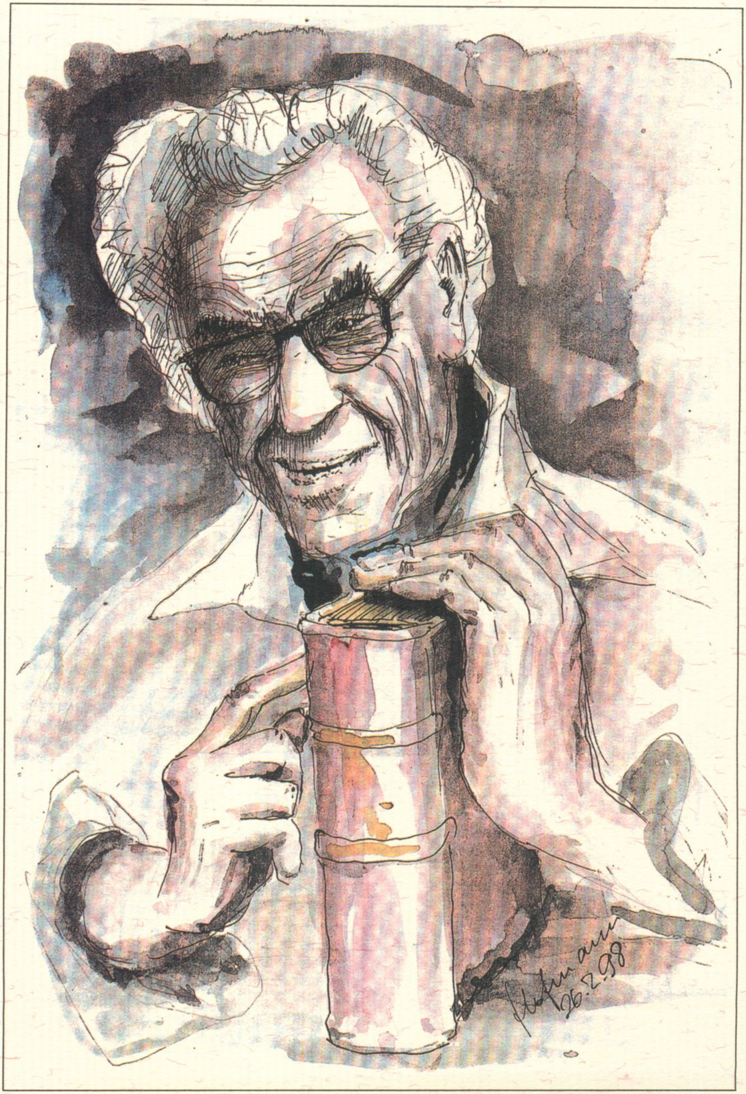
[5] P. エルデシュ：「ある組合せ問題 I」(*On a combinatorial problem I*), Nordisk Math. Tidskrift **11** (1963), 5-10.

[6] P. エルデシュ，R. K. ガイ：「交差数問題」(*Crossing number problems*), Amer. Math. Monthly **80** (1973), 52-58.

[7] P. エルデシュ，A. レニイ：「ランダムグラフの発展」(*On the evolution of random graphs*), Magyar Tud. Akad. Mat. Kut. Int. Közl. **5** (1960), 17-61.

[8] T. レイトン：『VLSI における複雑さの問題』(*Complexity Issues in VLSI*), MIT Press, Cambridge MA 1983.

[9] L. A. ゼケリー：「離散幾何における交差数と剛いエルデシュ問題」(*Crossing numbers and hard Erdős problems in discrete geometry*), Combinatorics, Probability, and Computing **6** (1997), 353-358.


26.2.98

図版について

本書を（ダームシュタットの）Karl Heinrich Hofmann が描いた素晴らしい絵で飾ることができたことは著者の喜びである．感謝する！

84 ページの正多面体と 97 ページのジャバラ運動を持つ球面の展開図は，（ウィーンの）WAF Ruppert による．

Jürgen Richter-Gebert は 87 ページの 2 つの図版を提供してくれた．

256 ページにはミネアポリスの Weisman 美術館の外観と平面図がある．その西の正面の写真は Chris Faust による．平面図はその西の正面の後ろにある Dolly Fiterman Riverview Gallery のものである．

ベルトラン，カントール，エルデシュ，オイラー，フェルマー，エルミート，ヘルダロッツ，ヒルベルト，ポーヤ，リトルウッド，シルヴェスターの肖像はオーベルヴォルファッハ数学研究所の写真アーカイブのものを（許しを得て）掲載した．（Annette Disch に感謝する！）

トゥラーンの肖像についてはヴェラ・ソスに感謝する．

エルミートの絵は彼の全集の第 1 巻から転載した．ビュフォンの肖像は MacTutor History of Mathematics のアーカイブのものである．

ケイリーの肖像は『ワイエルシュトラスのためのアルバム』(Photoalbum für Weierstraß)，Reinhard Bölling 編，Vieweg 1994 から，Kunstbibliothek, Staatliche Museen zu Berlin, Preussischer Kulturbesitz の許しを得て掲載した．

コーシーの肖像はパリのエコール・ポリテクニクのコレクションから許しを得て転載した．

フェルマーの絵は Stefan Hildebrandt と Anthony Tromba の著書『倹約家の（慎ましい）宇宙：自然界における形状』(The Parsimonious

Universe. Shape and Form in the Natural World), Springer-Verlag, New York 1996 から転載した.

エルンスト・ヴィットの肖像は Journal für die Reine und Angewandte Mathematik 誌の 426 巻 (1992) から Walter de Gruyter 出版社の許しを得て転載した. 1941 年頃に撮られたものである.

カロル・ボルスクの写真は 1967 年に Isaac Namioka によって撮影されたもので, 彼の親切な許しを得て掲載した.

（ブラウンシュヴァイクの）Peter Sperner 博士には, 父上の肖像の件で感謝する.

A. ニリーの肖像についてはノガ・アロンに感謝する.

クロード・シャノンの肖像は MIT の博物館から提供されたもので, その許可を得てここに掲載した.

人名索引

［訳者より］本文の人名に関し，原著の索引ではその記載ページを示すにとどめているが，日本語版では各人物について若干の注釈を訳者が加えることにした．訳者は，数学史の専門家ではないし，各人物（特に現役の人物）については，履歴・現職・専門分野など確認できないケースも少なからずあった．各注釈は，あくまでも本書の読者の便宜のために，訳者の判断で書いたものであるので，人物の記載に疎密が生じていることをお断りしておきたい．

生没年と生没地だけは記載したいものと調べてみたが，参考にした文献でもはっきりしていなかったり，矛盾することもある．その場合，明らかな誤りが認められる場合を除いて，記載が細かいものを掲載した．原則としては，『岩波数学辞典第 3 版』，大竹出版『世界数学者人名辞典』（A.L. ボロディーン，A.S. ブガーイ著，千田健吾，山崎昇訳），イギリスのセント・アンドリュース大学の数学史のホームページ MacTutor(http://www-groups.dcs.st-and.ac.uk/history) などを参照して，わかる限り記載しておいた．

また，各種受賞歴については，フィールズ賞についてのみ記載した．ここでは各人物に関する注釈は簡潔を旨としたが，訳者のホームページ（奥付参照）では，さらに詳しく雑多な話題を含んだバージョンを掲載している．各人物についてさらに知りたいと思われた読者は，ぜひこのホームページをご覧頂きたい．各人物の記載ページは各項目の末尾に示した．

事項索引

著　者

M. アイグナー (Martin Aigner)
Institut für Mathematik II
Freie Universität Berlin
Arnimallee 2
D-14195 Berlin, Germany
`http://www.math.fu-berlin.de/~aigner/`

G. M. ツィーグラー (Günter M. Ziegler)
Institut für Mathematik
Technische Universität Berlin
Straße des 17. Juni 136
10623 Berlin, Germany
`http://www.math.tu-berlin.de/~ziegler/`

訳　者

蟹江　幸博（かにえ　ゆきひろ）
'76 年 3 月，京都大学大学院理学研究科博士課程修了．
三重大学教育学部教授．理学博士．
専門：トポロジー，表現論．
訳書に，A.Ya. ヒンチン『数論の 3 つの真珠』（日本評論社），
H. ヴァルサー『黄金分割』（日本評論社），H. ヴァルサー『シンメトリー』（日本評論社），
V.I. アーノルド『古典力学の数学的方法』（共訳，岩波書店），
V.I. アーノルド『カタストロフ理論』（現代数学社），
V.I. アーノルド『数理解析のパイオニアたち』（シュプリンガー・フェアラーク東京），
E. ハイラー，G. ワナー『解析教程 上・下』（シュプリンガー・フェアラーク東京），
J.W. ミルナー『微分トポロジー講義』（シュプリンガー・フェアラーク東京），
G. トス『数学名所案内 上・下』（シュプリンガー・フェアラーク東京），
I.R. シャファレヴィッチ『代数学とは何か』（シュプリンガー・フェアラーク東京）．
`http://www.com.mie-u.ac.jp/~kanie/tosm/`

天書（てんしょ）の証明（しょうめい）　　　　定価（本体 3,500 円＋税）

発　行　2002 年 12 月 28 日（初版）
　　　　2004 年 9 月 17 日（初版 2 刷）
著　者　M. アイグナー，G. M. ツィーグラー
訳　者　蟹江 幸博
発行者　平野 皓正
発行所　シュプリンガー・フェアラーク東京株式会社
　　　　〒113-0033　東京都文京区本郷 3 丁目 3 番 13 号
　　　　TEL (03) 3812-0757 (営業直通)
印刷所　耕文社

ISBN 4-431-70986-X　C3041　　　　`http://www.springer-tokyo.co.jp`